VMware vCenter Configuration Manager Installation and Getting Started Guide

vCenter Configuration Manager 5.4.1

This document supports the version of each product listed and supports all subsequent versions until the document is replaced by a new edition. To check for more recent editions of this document, see http://www.vmware.com/support/pubs.

EN-000740-00

vmware

You can find the most up-to-date technical documentation on the VMware Web site at:
http://www.vmware.com/support/

The VMware Web site also provides the latest product updates.

If you have comments about this documentation, submit your feedback to:

docfeedback@vmware.com

© 2006-2011 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents.

VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

About This Book 9

Preparing for Installation 11
- **Installation Manager** 11
- **Installation Configurations** 12
- **Tools Installation** 12
- **General Prerequisites to Install VCM** 12
  - **Verify Hardware and Software Requirements** 12
  - **Verify Administration Rights** 12
  - **Set the Default Network Authority Account** 12
  - **Specify the Collector Services Account** 13
  - **Change the Collector Services Account Password in the Services Management Console** 13
  - **Change the Collector Services Account Password in the Component Services DCOM Config Console** 13
  - **Verify the VMware Application Services Account** 14
  - **Determine the VCM Remote Virtual Directory** 14
  - **Use Secure Communications Certificates** 14
  - **Understand Server Authentication** 14
  - **Verify the Foundation Checker System Checks** 16
  - **Install UNIX Patch for HP-UX 11.11** 16
- **VCM Uses FIPS Cryptography** 16
  - **VCM Uses Microsoft Cryptographic Service Providers for Windows Machines** 17
  - **Cryptography for UNIX/Linux Platforms** 17
  - **Cryptography used in VCM Software Components** 17
  - **Supported Windows and UNIX Platforms** 18

Installing VCM 19

Installing, Configuring, and Upgrading the OS Provisioning Server and Components 21
- **Restricted Network Environment** 21
- **Install and Configure the OS Provisioning Server** 21
  - **Install the OS Provisioning Server** 22
  - **Set the vcmuser Password** 24
  - **Configure DHCP** 25
  - **Configure TFTP** 26
  - **Create a Windows Boot Image** 26
  - **Copy the VCM Certificate to the OS Provisioning Server for Linux Provisioning** 27
  - **Configure OS Provisioning Server Integration with the VCM Collector** 28
- **Import Distributions into the OS Provisioning Server Repository** 33
  - **Create Directories for Windows Distributions** 34
  - **Import Windows Distributions** 34
  - **Import Linux/ESX Distributions** 36
  - **Using the basicimport Command Options** 38
- **Working with Custom Linux ISO Distributions** 38
- **Upgrade the OS Provisioning Server to 5.4.1** 39
  - **Before Upgrading the OS Provisioning Server** 39
  - **Upgrading the OS Provisioning Server** 39
  - **After Upgrading the OS Provisioning Server** 39
- **Managing the OS Provisioning Server System Logs** 40
- **ospctrl Command Options** 40

Upgrading or Migrating VCM 43
Upgrades 43
Migrations 43
Prerequisites to Migrate VCM 44
Back Up Your Databases 45
Back up Your Files 45
Export and Back up Your Certificates 45
Migrating VCM 46
Migrate Only Your Database 46
Replace Your Existing 32-Bit Environment with a Supported 64-bit Environment 47
Migrate a 32-bit Environment Running VCM 5.3 or Earlier to VCM 5.4.1 48
Migrate a 64-bit Environment Running VCM 5.3 or Earlier to VCM 5.4.1 49
Migrate a Split Installation of VCM 5.3 or Earlier to a Single-Server Installation 51
How to Recover Your Collector Machine if the Migration is not Successful 53
Upgrading VCM and Components 54
Upgrade VCM 55
Upgrade Existing Windows Agents 55
Upgrade Existing VCM Remote Clients 56
Upgrade Existing UNIX Agents 57
Upgrade VCM for Virtualization 60

Maintaining VCM After Installation 65
Customize VCM and Component-Specific Settings 65
Database Recovery Models 67
Configure Database File Growth 67
Configure Database Recovery Settings 68
Create a Maintenance Plan for SQL Server 2008 R2 69
Incorporate the VCM CMDB into your Backup and Disaster Recovery Plans 70

Getting Started with VCM Components and Tools 71
Understanding User Access 71
Running VCM as Administrator on the Collector 72
Log In to VCM 72
Getting Familiar with the Portal 73
General Information Bar 73
Portal Toolbar 74
Sliders 75

Getting Started with VCM 77
Discover, License, and Install Windows Machines 77
Discover, License, and Install Windows Machines 77
Verify Available Domains 78
Check the Network Authority 78
Assign Network Authority Accounts 79
Discover Windows Machines 79
License Windows Machines 80
Disable User Account Control for VCM Agent Installation 81
Install the VCM Windows Agent on Your Windows Machines 83
Enable UAC After VCM Agent Installation 89
Collect Windows Data 90
Windows Collection Results 91
Getting Started with Windows Custom Information 92
Discover, License, and Install UNIX/Linux Machines 111
Upgrade Requirements for UNIX/Linux Machines 112
Add UNIX/Linux Machines 112
License UNIX/Linux Machines 114
Install the Agent on UNIX/Linux Machines 114

Collect UNIX/Linux Data 121
UNIX/Linux Collection Results 121
Discover, License, and Install Mac OS X Machines 122
Add Mac OS X Machines 123
License Mac OS X Machines 124
Install the Agent on Mac OS X Machines 124
Collect Mac OS X Data 129
Mac OS X Collection Results 131
Discover, Configure, and Collect Oracle Data from UNIX Machines 131
Discover Oracle Instances 132
Edit Oracle Instances 133
Collect Oracle Data 137
Oracle Collection Results 138
Customize VCM for your Environment 139
How to Set Up and Use VCM Auditing 139

Getting Started with VCM for Virtualization 141
Virtual Environments Configuration 141
ESX/ESXi Server Collections 142
vCenter Server Collections 143
vCloud Director vApp Virtual Machines Collections 143
Configure vCenter Server Data Collections 143
Configure vCenter Server Collection Prerequisites 143
Collect vCenter Server Data 145
vCenter Server Collection Results 146
Troubleshooting vCenter Server Data Collections 146
Configure Virtual Machine Host Collections 147
vCenter Server Collection Upgrade Considerations 147
Configure the Collector as an Agent Proxy 147
License and Configure Virtual Machine Hosts 148
Copy Files to the ESX/ESXi Servers 150
Collect Virtualization Data 151
Virtualization Collection Results 152
Configure vCloud Director vApp Virtual Machines Collections 152
Network Address Translation and vCloud Director vApp Discovery Rules 153
Generate vCloud Director Collection Credentials 155
Create vCloud Director Data Collection Filters 156
Collect vCloud Director Data 158
Discover vCloud Director vApp Virtual Machines 158
vCloud Director Collection Results 162
Configure the vSphere Client VCM Plug-In 163
Register the vSphere Client VCM Plug-In 163
Configuring the vSphere Client VCM Plug-In Integration Settings 164
Manage Machines from the vSphere Client 165
Troubleshooting the vSphere Client VCM Plug-In Registration 165

Getting Started with VCM Remote 167
VCM Remote Management Workflow 167
Configuring VCM Remote Connection Types 167
Using Certificates With VCM Remote 168
Configure and Install the VCM Remote Client 168
Configure the VCM Remote Settings 168
Install the VCM Remote Client 171
Connect VCM Remote Client Machines to the Network 178
VCM Remote Collection Results 179

Getting Started with VCM Patching 181

VCM Patching for Windows and UNIX/Linux Machines 181
VCM Patching for Windows Machines 181
VCM Patching for UNIX and Linux Machines 182
Minimum System Requirements 182
UNIX and Linux Patch Assessment and Deployment 182
Getting Started with VCM Patching 184
vCenter Software Content Repository Tool 190
Running VCM Patching Reports 197
Customize Your Environment for VCM Patching 198

Getting Started with Operating System Provisioning 199
OS Provisioning Components 199
How OS Provisioning Works 200
Provision Target Machines with Operating System Distributions 201
Collect OS Distributions 201
Discover Provisionable Machines 202
Provision Machines with Operating System Distributions 202
Provisioned Machines Results 213
Re-Provision Machines 214

Getting Started with Software Provisioning 217
Using Package Studio to Create Software Packages and Publish to Repositories 217
Software Repository for Windows 217
Package Manager for Windows 217
Software Provisioning Component Relationships 218
Install the Software Provisioning Components 218
Install Software Repository for Windows 219
Install Package Studio 220
Install Package Manager on Managed Machines 222
Using Package Studio to Create Software Packages and Publish to Repositories 223
Creating Packages 223
Using VCM Software Provisioning for Windows 225
Collect Package Manager Information from Machines 226
Collect Software Repository Data 226
Add Repository Sources to Package Managers 227
Install Packages 228
Related Software Provisioning Actions 230
Viewing Provisioning Jobs in the Job Manager 230
Create Compliance Rules Based on Software Provisioning Data 231
Create Compliance Rules Containing Software Provisioning Remediation Actions 232

Getting Started with VCM Management Extensions for Assets 235
Configure Asset Data Fields 235
Review Available Asset Data Fields 236
Add an Asset Data Field 236
Edit an Asset Data Field 237
Delete a VCMMXA Data Field 238
Change the Order of Asset Data Columns 238
Refresh Dynamic Asset Data Fields 239
Configure Asset Data Values for VCM Machines 239
Configure Asset Data for Other Hardware Devices 240
Add Other Hardware Devices 240
Add Multiple Similar Other Hardware Devices 241
Edit Asset Data for Other Hardware Devices 241
Edit Asset Data Values for Other Hardware Devices 242
Delete Other Hardware Devices 242
Configure Asset Data for Software 243

Add Software Assets 243
Add Multiple Similar Software Assets 244
Edit Asset Data for Software 245
Edit Asset Data Values for Software 245
Delete Software Data 246

Getting Started with VCM Service Desk Integration 247
Configure Service Desk Integration 247
View Service Desk Integration in the Console 247
View Service Desk Integration in Job Manager 248

Getting Started with VCM for Active Directory 249
Configure Domain Controllers 249
Verify Available Domains 250
Check the Network Authority Account 250
Assign Network Authority Accounts 251
Discover Domain Controllers 251
License Domain Controllers 252
Install the VCM Windows Agent on Your Domain Controllers 253
Collect Domain Controller Data 254
Configure VCM for Active Directory as an Additional Product 255
Install VCM for Active Directory on the Domain Controllers 255
Run the Determine Forest Action 256
Run the Domain Controller Setup Action 256
Collect Active Directory Data 257
Active Directory Collection Results 258

Installing and Getting Started with VCM Tools 261
Install the VCM Tools Only 261
VCM Import/Export and Content Wizard Tools 262
Run the Import/Export Tool 263
Run the Content Wizard to Access Additional Compliance Content 263
Run the Deployment Utility 263
Package Studio 264
Foundation Checker 264

Index 265

About This Book

The *VMware vCenter Configuration Manager Installation and Getting Started Guide* describes the steps necessary for a successful VCM installation.

This document contains the following information:

- Preparing for the VCM installation
- Installing VCM
- Maintaining VCM after installation
- Getting started with VCM and its components

Read this document and complete the associated procedures to prepare for a successful installation.

The *VMware vCenter Configuration Manager Installation and Getting Started Guide* applies to VCM, Foundation Checker, and Service Desk Connector.

Intended Audience

This information is written for experienced Windows or UNIX/Linux/Mac OS X system administrators who are familiar with managing network users and resources and with performing system maintenance.

To use this information effectively, you must have a basic understanding of how to configure network resources, install software, and administer operating systems. You also need to fully understand your network's topology and resource naming conventions.

Document Feedback

VMware welcomes your suggestions for improving our documentation. If you have comments, send your feedback to docfeedback@vmware.com.

VMware VCM Documentation

The vCenter Configuration Manager (VCM) documentation consists of the *VCM Hardware and Software Requirements Guide*, *VCM Foundation Checker User's Guide*, *VCM Installation and Getting Started Guide*, *VCM Troubleshooting Guide*, VCM online Help, and other associated documentation.

Technical Support and Education Resources

The following technical support resources are available to you. To access the current version of this book and other books, go to http://www.vmware.com/support/pubs.

Online and Telephone Support

To use online support to submit technical support requests, view your product and contract information, and register your products, go to http://www.vmware.com/support.

Customers with appropriate support contracts should use telephone support for priority 1 issues. Go to http://www.vmware.com/support/phone_support.html.

Support Offerings

To find out how VMware support offerings can help meet your business needs, go to http://www.vmware.com/support/services.

VMware Professional Services

VMware Education Services courses offer extensive hands-on labs, case study examples, and course materials designed to be used as on-the-job reference tools. Courses are available onsite, in the classroom, and live online. For onsite pilot programs and implementation best practices, VMware Consulting Services provides offerings to help you assess, plan, build, and manage your virtual environment. To access information about education classes, certification programs, and consulting services, go to http://www.vmware.com/services.

1 Preparing for Installation

You must prepare your environment before you install VCM components and tools.

Prerequisites

- Verify that your environment meets the security requirements. See the *VCM Security Environment Requirements White Paper* on the Download VMware vCenter Configuration Manager Web site.
- Verify that your hardware and software configuration meets the requirements to install VCM. See the *VCM Hardware and Software Requirements Guide*.
- Verify that your hardware and software meet the requirements to install VCM and install and run the standalone VCM Foundation Checker. See "Installing and Getting Started with VCM Tools" on page 261.

To prepare your environment, familiarize yourself with the following topics.

- Installation Manager: Installs and activates VCM components and tools.
- Installation Configurations: Describes supported installation configurations.
- Tools Installation: Lists the installed VCM tools.
- General Prerequisites to install VCM: Describes prerequisites that you must perform before you install VCM.

Installation Manager

The VCM Installation Manager installs new versions of VCM components and tools and upgrades existing versions. Installation Manager performs several actions.

- Checks managed machines to ensure that they meet the hardware and software prerequisites for the installation.
- Confirms the license file that you apply during the installation.
- Installs the components and tools in the appropriate order on your machines.
- Tests each installation step to verify that all components install successfully and that licensed components activate successfully.

Installation Manager operates with minimal user input and reports on progress during the installation process. All VCM components are installed. Only components that you purchased are licensed. You can purchase more licenses later to activate the additional installed components.

If you are upgrading, see "Upgrading or Migrating VCM" on page 43.

Installation Configurations

Understand the installation configurations, configure your hardware, and install the prerequisite software. See the *VCM Hardware and Software Requirements Guide*.

Split installations are not supported. To migrate a split installation of VCM 5.3 or earlier to a single-server installation, see "Upgrading or Migrating VCM" on page 43. For more information, contact VMware Technical Support.

Tools Installation

The VCM Installation Manager installs several tools.

- Foundation Checker
- Import/Export Tool and Content Wizard Tool
- Package Studio

You may install VCM tools separately on a non-Collector machine. See "Installing and Getting Started with VCM Tools" on page 261.

General Prerequisites to Install VCM

Perform the general prerequisites to ensure that your environment is adequately prepared before you use Installation Manager to install VCM.

Verify Hardware and Software Requirements

Your hardware and software configuration must meet the requirements in the *VCM Hardware and Software Requirements Guide*.

Verify Administration Rights

Verify that the user account of the person who performs the installation or upgrade has all of the following rights.

- System administrator on the machines on which the installation or upgrade is performed, **and**
- System administrator on the database instance to be used, **and**
- Member of a domain.

The installing user account must **not** be the account used to run SQL Server services. In addition, after installation, do not create a VCM user that uses the SQL Server services account credentials.

Set the Default Network Authority Account

Define the network authority account in the Local Administrators group on each Collector machine before you install VCM. See the *VCM Hardware and Software Requirements Guide*.

You specify the default network authority account during VCM installation. The default network authority account can be a system administrator account, such as a Domain Admin in the Local Admin Group.

The Local System account, `NT AUTHORITY\System`, has unrestricted access to all local system resources. This account is a member of the Windows Administrators group on the local machine and a member of the SQL Server `sysadmin` fixed server role.

If the `NT AUTHORITY\System` account does not have access to the VCM installation binary files, the installation results in an "access denied" error. You must grant access to the `NT AUTHORITY\System` account from the installation source directory and then run the installation again. Right-click the folder, select the Security tab, and verify that the user or user's group has Full Control of the file/folder.

To change the network authority account later in VCM, click **Administration** and select **Settings > Network Authority**.

Specify the Collector Services Account

You specify the Collector Services Account during VCM installation. The account can be a system administrator account and must exist in the Local Administrators group on the Collector machine. The account must **not** be the Local System account.

If the password for the account changes, you must change the password in the Services Management console and the Component Services DCOM Config console.

Change the Collector Services Account Password in the Services Management Console

If the password for your Collector services account changes, you must change the services password in the Services Management Console.

Procedure

1. Click **Start**.
2. Select **All Programs > Administrative Tools > Services**.
3. Locate all of the services that use the collector services account to log on.
4. Right-click each of these services and select **Properties**.
5. Click the **Log On** tab and update the password field to reflect your new password.
6. Click **OK**.

Change the Collector Services Account Password in the Component Services DCOM Config Console

If the password for your Collector services account changes, you must change the services password in the Component Services DCOM Config console.

Procedure

1. Click **Start**.
2. Select **All Programs > Administrative Tools > Component Services**.
3. Expand **Component Services** and **Computers**.
4. Expand **My Computer** and select **DCOM Config**.
5. Right click **LicenseDcom** and select **Properties**.
6. Click the **Identity** tab and update the password field to reflect your new password.
7. Click **OK**.

Verify the VMware Application Services Account

Verify that the VMware Application Services Account is a domain user. This account has full administrative authority for the CSI_Domain database.

IMPORTANT Never use this account as a VCM login or for any other purpose.

Determine the VCM Remote Virtual Directory

You specify the VCM Remote Virtual Directory during VCM installation. You can change the account later using the IIS Management console.

IMPORTANT When you specify the VCM Remote Virtual Directory, to minimize security risks to your accounts, always use an account that differs from the account used for your Default Network Authority Account or your Services Account.

Use Secure Communications Certificates

VCM uses Transport Layer Security (TLS) to secure all HTTP communication with all Windows Agents and UNIX Agents in HTTP mode. TLS uses certificates to authenticate the Collector and Agents to each other. During VCM installation, you must specify the Collector and Enterprise certificates. If you use your own certificates, you must familiarize yourself with the certificate names in advance so that you can select them during installation.

A valid Collector certificate must be:

- Located in the local machine personal certificate store.
- Valid for Server Authentication. If any Enhanced Key Usage extension or property is present, it must include the Server Authentication `OID 1.3.6.1.5.5.7.3.1`. If the Key Usage extension is present, it must include `DIGITAL_SIGNATURE`.
- Active, and not expired.

If you do not want to use your own certificates, you can have Installation Manager generate the Collector and Enterprise certificates for you, select the **Generate** option during the installation.

If you install more than one Collector that will communicate with the same Agent(s), or if you plan to replace or renew your certificates later, you must follow the special considerations to generate and select certificates in VCM Installation Manager. See the *Transport Layer Security Implementation for VCM* white paper on the Download VMware vCenter Configuration Manager Web site.

Understand Server Authentication

VCM supports Server Authentication, which is a method to authenticate the server to the client. In VCM environments where TLS is used, VCM Agents verify the identity of the Collectors by using and verifying certificates over HTTP.

The server typically authenticates a client or user by requiring information such as a user name and password. When Server Authentication is used, the client or user verifies that the server is valid. To accomplish this verification, the server provides a certificate issued by a trusted authority, such as Verisign. If your client Web browser has the Verisign Certified Authority certificate in its trusted store, the Web browser can trust that the server is actually the Web site you access.

To guarantee the identity of servers and clients, TLS uses certificates that are managed by a public key infrastructure (PKI). A certificate is a package that contains a public key, information that identifies the owner and source of that key, and one or more certifications (signatures) to verify that the package is authentic. To sign a certificate, an issuer adds information about itself to the information that is already contained in the certificate request. The public key and identifying information are hashed and signed using the private key of the issuer's certificate.

Certificates are defined by the X.509 RFC standard, which includes fields that form a contract between the creator and consumer. The Enhanced Key Usage extension specifies the use for which the certificate is valid, including Server Authentication.

Enterprise and Collector Certificates

An Enterprise Certificate and one or more Collector Certificates enable secure HTTP Collector and Agent communication in VCM. The Enterprise Certificate enables VCM to operate in a multi-Collector environment. Agents have the Enterprise Certificate in their trusted certificate stores, and they use the Enterprise Certificate to validate any certificate issued by the Enterprise Certificate. All Collector Certificates are expected to be issued by the Enterprise Certificate, which is critical in environments where a single Agent is shared between two Collectors.

Server authentication is required to establish a TLS connection with an Agent. All VCM Collectors should have a common Enterprise Certificate. Each Collector Certificate is issued by the Enterprise Certificate, and is capable of Server Authentication. Collector Certificates in VCM must adhere to the requirements for secure communications certificates. See "General Prerequisites to Install VCM" on page 12.

- The Collector Certificate initiates and secures a TLS communication channel with an HTTP Agent. The Agent must be able to establish that the Collector Certificate can be trusted, which means that the Collector Certificate is valid and the certification path starting with the Collector Certificate ends with a trusted certificate. By design, the Enterprise Certificate is installed in the Agent's trusted store. The trust chain ends with the Enterprise Certificate.
- A Collector Certificate can issue Agent certificates. When all Collector Certificates are issued by the same Enterprise Certificate, any Agent Certificate may be issued by any Collector Certificate, and all Agents can trust all Collectors. All Collectors can validate all Agent Certificates. Agent Certificates are used for Mutual Authentication only. VCM supports Mutual Authentication, which requires interaction with VMware Technical Support and a Collector Certificate that has certificate signing capability.
- The Collector Certificate and associated private key must be available to the Collector. This certificate is stored in the local machine personal system store.

Delivering Initial Certificates to Agents

VCM Agents use the Enterprise Certificate to validate Collector Certificates. The Agent must have access to the Enterprise Certificate as a trusted certificate. In most cases, VCM delivers and installs the Enterprise Certificate as needed.

- Installing the Agent from a Disk (Windows only)

  The VCM Installation DVD does not contain customer-specific certificates. If HTTP is specified, the manual VCM installer requests the location of the Enterprise Certificate file during the installation. You must have the Enterprise Certificate file available at installation time. You can copy the certificate file, which has a `.pem` extension, from the `CollectorData` folder on the Collector. You must copy the certificate file when you run the manual installer directly using `CMAgentInstall.exe` or when you use the **Agent Only** option in the DVD auto-run program.
- Using `CMAgentInstall.exe` to Install the Agent (Windows only)

The `CMAgentInstall.exe` or `CMAgent[version].msi` is the manual Agent installer program. The manual installer requests the location of the Enterprise Certificate file when HTTP is specified. You must have the Enterprise Certificate file available at installation time. You can copy the certificate file from the `CollectorData` folder on the Collector.

- Using the MSI Install Package

  When you specify HTTP, the MSI Agent install package also requires access to the `.pem` file.

- Installing the Agent for UNIX/Linux

  See "Install the Agent on UNIX/Linux Machines" on page 114.

Installing the Agent Using a Provisioning System

For Windows, the manual installation program is available in EXE and MSI formats. Both versions allow you to specify the Enterprise Certificate file by using a command line switch. You may omit the certificate installation step by using a command line switch.

When these programs are run through a provisioning system, you must ensure that the Enterprise Certificate is available and secure, and configure the program options appropriately. Alternatively, you may choose to send the Enterprise Certificate to Agents by some other means and configure the provisioning system to omit certificate installation.

For UNIX/Linux, each UNIX/Linux installation package is targeted for one or more supported platforms. To install the UNIX/Linux Agent using a provisioning system, extract the installation package and then deploy the extracted file with the provisioning system. The Enterprise Certificate is embedded in the installation package on the Collector.

For more information about installing the Agent on UNIX/Linux machines, and UNIX/Linux packages and platforms, see "Install the Agent on UNIX/Linux Machines" on page 114.

Verify the Foundation Checker System Checks

Installation Manager runs Foundation Checker automatically during the VCM installation. Foundation Checker checks your Collector to verify that all of the prerequisites are satisfied for a successful installation.

When Foundation Checker runs as part of the Installation Manager process, it verifies component-specific issues against VCM. Foundation Checker captures common issues that are difficult to remediate and identifies issues with the components and version of VCM being installed. Foundation Checker must run without generating errors before you install VCM. For more information about the standalone Foundation Checker, see "Installing and Getting Started with VCM Tools" on page 261) and the *VCM Foundation Checker User's Guide* on the Download VMware vCenter Configuration Manager Web site.

Install UNIX Patch for HP-UX 11.11

If you install the VCM Agent on HP-UX 11.11 platforms, install patch `PHSS_30966`. For assistance, contact VMware Technical Support.

VCM Uses FIPS Cryptography

VCM incorporates cryptographic service providers that conform to Federal Information Processing Standards (FIPS) standards. The FIPS standards are developed by the US National Institute of Standards (NIST) and the Canadian Communications Security Establishment (CSE).

VCM supports the following FIPS standards.

- FIPS 140-2: Security Requirements for Cryptographic Modules
- FIPS 46-3: Data Encryption Standard (DES)
- FIPS 81: DES Modes of Operation
- FIPS 113: Computer Data Authentication
- FIPS 171: Key Management
- FIPS 180-1: Secure Hash Standard (SHA-1)
- FIPS 186-2: Digital Signature Standard (DSA) and Random Number Generation (RNG)
- FIPS 198: Message Authentication Codes (MACs) using SHA-1
- FIPS 197: Advanced Encryption Standard (AES) Cipher
- FIPS 200: Federal Information Security Management Act (FISMA)
- SP 800-2: Public Key Cryptography (including RSA)
- SP 800-20: Triple DES Encryption (3DES) Cipher

VCM Uses Microsoft Cryptographic Service Providers for Windows Machines

On Windows machines, VCM uses cryptography using the Microsoft CryptoAPI, which is a framework that dispatches to Microsoft Cryptographic Service Providers (CSPs). CSPs are not shipped with VCM or installed by VCM, but instead are part of the security environment that is included with Microsoft Windows. In the configurations supported by VCM, these CSPs are FIPS 140-2 validated.

For a current table of FIPS certificate numbers, see the FIPS 140 Evaluation in the online Microsoft Library.

Cryptography for UNIX/Linux Platforms

On UNIX/Linux platforms, the VCM Agent uses the cryptography of the OpenSSL v0.9.7 module. This cryptographic library is installed with the VCM Agent.

Cryptography used in VCM Software Components

VCM uses software components that also use cryptography.

- Microsoft IIS, Internet Explorer, and SChannel (SSL/TLS) systems call the CryptoAPI, and therefore use the Windows FIPS-validated modules.
- VCM for Virtualization uses ActiveX COM components from WeOnlyDo! Software (WOD) for SSH and SFTP services.
- WOD uses the FIPS 140-2 compliant OpenSSL library.

Table 1–1. Installed or Used Crytography Modules

System	Platform	Open SSLFIPS 1.1.2	Open SSLFIPS 1.1.1	Open SSLCrypt 0.9.7	Crypto++	Crypto API
UI	Windows					Used
VCMServer	Windows				Installed	Used
Virt Proxy	Windows	Installed				Used
AD Agent	Windows					Used
Win Agent	Windows					Used

System	Platform	Open SSLFIPS 1.1.2	Open SSLFIPS 1.1.1	Open SSLCrypt 0.9.7	Crypto++	Crypto API
UNIX Agent	HP/UX			Installed	Installed	
	AIX			Installed	Installed	
	Solaris			Installed	Installed	
	Debian		Installed		Installed	
	Red Hat		Installed		Installed	
	SUSE		Installed		Installed	
ESX Server	All	No cryptography modules are used or installed on ESX.				

Supported Windows and UNIX Platforms

For a list of supported Windows and UNIX platforms and architectures, see the *VCM Hardware and Software Requirements Guide*. For information about TLS, see the *Transport Layer Security (TLS) Implementation for VCM* white paper on the Download VMware vCenter Configuration Manager Web site.

Installing VCM

2

Use Installation Manager to install VCM and all of its components and tools. To install only the VCM tools, see "Installing and Getting Started with VCM Tools" on page 261.

The VMware vCenter Configuration Manager (VCM) Installation Manager is a standalone application that checks your machine to confirm that it is properly configured, installs VCM, and configures licensed components during the installation process.

VCM 5.4.1 supports 64-bit environments that include 64-bit hardware, the 64-bit Windows Server 2008 R2 operating system, and SQL Server 2008 R2.

When you install VCM and related components, the default settings might not fit your configuration exactly. You must read the information that appears for each configurable component and supply the appropriate information. If you migrate VCM or SQL Server, or migrate to a 64-bit system, see "Upgrading or Migrating VCM" on page 43.

CAUTION The installation process adds the `%windir%\Installer\` folder, which contains VCM related MSI files. Do not move or delete the content of this folder. If you delete the content, you will not be able to use Installation Manager to upgrade, repair, or uninstall VCM.

Prerequisites

- Review the list of supported platforms in the *VCM Hardware and Software Requirements Guide*.
- Before you migrate VCM to VCM 5.4.1, read Migrating VCM and Related Components.

Procedure

1. To install VCM, insert the installation disk into the Windows machine.

   The initial installation screen appears and displays several options. If the installation screen does not appear automatically, or if you began the installation from a network location, navigate to the disk root directory or the file share and double-click `setup.exe`.

2. Select an installation option.

Option	Description
Run Installation Manager	Starts Installation Manager and begins the installation.
View Help	Displays the Installation Manager Help, which describes the selections that appear during the installation.
Browse Contents of Installation CD	Starts Windows Explorer and displays the content of the installation disk, which includes documentation.
Contact Support Team	Displays instructions to contact VMware Technical Support.
Exit	Closes Installation Manager.

3. Follow the steps through the wizard to complete the installation.

   For details about the installation options, open the Installation Manager online help.

What to do next

When the installation is finished, configure SQL Server database file growth and database recovery settings to tune your VCM database. See "Maintaining VCM After Installation" on page 65.

Installing, Configuring, and Upgrading the OS Provisioning Server and Components

3

The Operating System (OS) Provisioning Server serves as a repository of imported OS distributions and manages the installation of the distributions on target machines. The installation of the distributions is part of the OS provisioning function in VCM, which identifies machines that can be provisioned and initiates the OS provisioning on the target machines.

You install and configure the OS Provisioning Server on a Red Hat server. After configuring the server, you import the operating system ISO files. The database manages the metadata about the OS distributions and the ISO files are saved in the OS Provisioning Server repository. After you import the distributions, the server performs the installation process, which is managed in VCM. See "Getting Started with Operating System Provisioning" on page 199 for provisioning machines instructions.

You cannot directly upgrade from OS Provisioning Server 5.4 to 5.4.1. Nor is OS Provisioning Server 5.4 compatible with VCM 5.4.1. You must install the new 5.4.1 OS Provisioning Server components, configure the server, and import the operating system ISO files into the new database structure. See "Upgrade the OS Provisioning Server to 5.4.1" on page 39.

When the OS Provisioning Server is installed and configured, consult the *VCM Backup and Disaster Recovery Guide* and create a backup plan for your server and files.

Troubleshooting information is available in the *VCM Troubleshooting Guide*.

Restricted Network Environment

To maintain security during the OS provisioning process, install and run your OS Provisioning Server in a private or restricted network. When you provision target machines, you connect the machines to this private network. See VCM Security Environment Requirements.

Install and Configure the OS Provisioning Server

You install the OS Provisioning Server and configure the components used to manage your operating system distributions. After you configure the components, you import the distributions and use VCM to install them on target machines.

Procedure

1. "Install the OS Provisioning Server" on page 22

   Using the supplied media or media images, install the OS Provisioning Server and run the command to create the distribution repository.

2. "Set the vcmuser Password" on page 24

   Configure the `vcmuser` to use when you import distributions into the OS Provisioning Server repository and for communication between VCM and the OS Provisioning Server.

3. "Configure DHCP" on page 25

   When you configure a private, isolated network that is used specifically for provisioning, the OS Provisioning Server uses the DHCP server it installed to provide addresses and network boot information to nodes connected to the network.

4. "Configure TFTP " on page 26

   The OS Provisioning Server provides TFTP services that run on the provisioning network. You must configure the TFTP server to listen on the private OS provisioning network interface.

5. "Create a Windows Boot Image" on page 26

   Create a Windows boot image and copy it to the OS Provisioning Server. You create the image on a Windows 2008 or Windows 7 machine, and copy the files to the OS Provisioning Server.

6. "Copy the VCM Certificate to the OS Provisioning Server for Linux Provisioning" on page 27

   If you use the OS Provisioning Server to install Linux distributions, you must copy the VCM certificate file to the OS Provisioning Server to ensure the certificate is included with the Agent when OS Provisioning Server creates the configured session prior to provisioning.

7. "Configure OS Provisioning Server Integration with the VCM Collector" on page 28

   The integration between VCM and the OS Provisioning Server uses Stunnel to establish secure communication between and the SOAP services of the two components.

Install the OS Provisioning Server

Using the supplied media or media images, install the OS Provisioning Server and run the command to create the distribution repository.

VCM OS provisioning supports a single instance of VCM with a single instance of the OS Provisioning Server.

Prerequisites

- Install VCM. See "Installing VCM" on page 19.
- Ensure the target machine meets the prerequisites specified in the *VCM Hardware and Software Requirements Guide*.
- Determine whether you are installing the OS Provisioning Server as an attended or unattended installation. To run an unattended installation, use the `./autoinstall -a y` command. This procedure is based on an attended installation.

Procedure

1. On the target machine, log in as `root`.
2. Mount the `VCM-OS-Provisioning-Server-<version number>.iso` by attaching or mounting the image.

   When you mount the image, do not use the `no exec` option.
3. Type `cd /<path to mounted OS Provisioning Server.iso>` to change the directory to the location of the image.
4. Run the `./INSTALL-ME` command to install server.
5. In the Nixstaller window, click **Next**.
6. In the dialog box, click **Continue**.
7. In the dialog box, click **Close** when the installation finishes.
8. In the Nixstaller window, click **Finish**.
9. Run the `service FastScale status` command to verify that the installation completed successfully.

   A successful installation displays the following results. PID values vary.

   ```
   rsyslogd (pid 3335) is running...
   fsmesgd (pid 3517) is running...
   fsrepod (pid 3683) is running...
   fsadmin (pid 12618) is running...
   dhcpd is stopped
   tftpd (pid 12057) is running
   fsjobd (pid 4237) is running...
   fshinvd (pid 4249) is stopped...
   stunnel (pid 4262 4261 4260 4259 4258 4257) is running...
   ```

   An unsuccessful installation displays `FastScale: unrecognized service` or several of the above mentioned services are not running. Review the logs to determine possible problems.
10. Run the `/opt/FastScale/sbin/create-repository` command.

    This action updates the repository database and destroys any existing repository information
11. Reboot the OS Provisioning Server to ensure that all related services are started in the correct order.
12. Run the `service FastScale status` command to verify the OS Provisioning Server services after reboot.

    A successful installation displays the services and their PIDs as running.

What to do next

- To ensure proper security, you must set the password for the vcmuser. See "Set the vcmuser Password" on page 24.
- (Optional) Add the OS Provisioning Server maintenance commands to the root user's path. The OS Provisioning Server modifies the default shell profiles by adding `/opt/FastScale/sbin` to the `root` account. When the user is `root`, the maintenance commands in `/opt/FastScale/sbin` are available in the default path and are available when the profile is reloaded.

Uninstall the OS Provisioning Server

Uninstalling the OS Provisioning Server removes the provisioning application from the machine on which it is installed. You must mount the OS Provisioning Server media and run the uninstall command.

CAUTION The uninstall process removes the application and deletes all the data in the database.

Procedure

1. On the OS Provisioning Server, log in as `root`.
2. Mount the OS Provisioning Server ISO by attaching or mounting the image.
3. Type `cd /<path to OS Provisioning Server.iso>` to change the directory to the location of the image.
4. Run the `./UNINSTALL-ME` command to uninstall the application.
5. Type `yes`.

   The uninstall process completes and generates a log. See the example log.

```
[Thu Jul 22 08:57:06 IST 2010] UNINSTALL-ME: Starting uninstallation of VCM OS Provisioning Server...

[Thu Jul 22 08:57:08 IST 2010] UNINSTALL-ME: FastScale service is running

[Thu Jul 22 08:57:08 IST 2010] UNINSTALL-ME: Stopping FastScale service

[Thu Jul 22 08:57:08 IST 2010] UNINSTALL-ME: Command : /sbin/service FastScale stop

Shutting down FSnetfs: [ OK ]

Shutting down FSsyslog: [ OK ]

Shutting down FSmesgd: [ OK ]

Shutting down FSdhcpd: [ OK ]

..........

[Thu Jul 22 09:00:44 IST 2010] UNINSTALL-ME: Uninstallation complete!
```

Set the vcmuser Password

Configure the `vcmuser` to use when you import distributions into the OS Provisioning Server repository and for communication between VCM and the OS Provisioning Server.

Do not delete the user or change the permissions, but you must set the `vcmuser` password based on your corporate standards.

Prerequisites

Verify that the OS Provisioning Server is installed. See "Install the OS Provisioning Server" on page 22.

Procedure

1. On the OS Provisioning Server, log in as `root`.
2. Run the `passwd vcmuser` command.
3. Type and confirm the new password.

What to do next

Configure DHCP with your local settings. See "Configure DHCP" on page 25.

Configure DHCP

When you configure a private, isolated network that is used specifically for provisioning, the OS Provisioning Server uses the DHCP server it installed to provide addresses and network boot information to nodes connected to the network.

Prerequisites

Determine whether you are using a private network (recommended) or shared network (supported, but not recommended). If you are provisioning systems on a shared network, you probably have a DHCP server on the network. Disable the OS Provisioning Server's DHCP server and configure your regular DHCP server to provide network boot information for machines to be provisioned. See "Configure a DHCP Server Other Than the OS Provisioning Server" on page 25 .

Procedure

1. Open `/opt/FastScale/etc/dhcpd.conf`.
2. Configure the settings for your environment.

Option	Description
`subnet`	The IP address subnet of the private network interface. Default value is 10.11.12.0.
`netmask`	The netmask of the subnet. Default value is 255.255.255.0.
`range`	The range of allocated IP addresses for the provisioned nodes. Default value is 10.11.12.100–10.11.12.200.
`broadcast-address`	The broadcast address on the subnet. Default value is 10.11.12.255.
`next-server`	The IP address of the private network interface. Default value is 10.11.12.1.

What to do next

Configure the TFTP server to work with the provisioning environment. See "Configure TFTP " on page 26.

Configure a DHCP Server Other Than the OS Provisioning Server

To configure your system to work with a DHCP server other than the one on the OS Provisioning Server, you turn off the OS Provisioning Server DHCP server and configure your corporate DHCP server to connect to the OS Provisioning Server after nodes connect and NetBoot (PXE) starts. The nodes download the boot kernel from the OS Provisioning Server through TFTP.

Procedure

1. On the OS Provisioning Server, log in as `root`.
2. Open `/etc/sysconfig/FSdhcpd`.
3. Change `DHCPD_CONF=/opt/FastScale/etc/dhcpd.conf` to `DHCPD_CONF=/opt/FastScale/etc/dhcpd.conf.none`

   This change prevents the DHCP from resetting after a reboot.

4. Run the `/opt/FastScale/etc/init.d/FSdhcpd stop` command.
5. On the corporate DHCP server, update `dhcpd.conf` to add these options:

```
allow bootp;

allow booting;

next-server <IP address of the OS Provisioning Server>;
```

Configure TFTP

The OS Provisioning Server provides TFTP services that run on the provisioning network. You must configure the TFTP server to listen on the private OS provisioning network interface.

Procedure

1. On the OS Provisioning Server, log in as `root`.
2. Run `ospctrl --showconfig`.

   The following results verify that the TFTP and Apache services are running.

```
TFTP - Configured on * - Running

Apache - Configured on * - Running
```

3. Run `ospctrl --configure --privateip <IP Address>`.

   The configuration process runs. The IP address is 10.11.12.1.

```
Shutting down FStftpd: [ OK ]

Starting FStftpd: [ OK ]

TFTP - Configured on 10.11.12.1 - Running

Shutting down FSadmin: [ OK ]

Starting FSadmin: [ OK ]

Apache - Configured on 10.11.12.1 - Running
```

4. Run `ospctrl --showconfig`.

   The following text appears when the TFTP and Apache services are running.

```
TFTP - Configured on 10.11.12.1 - Running

Apache - Configured on 10.11.12.1 - Running
```

What to do next

To install Windows distributions on target machines, you must create a Windows boot image and copy it to the OS Provisioning Server. See "Create a Windows Boot Image" on page 26.

Create a Windows Boot Image

Create a Windows boot image and copy it to the OS Provisioning Server. You create the image on a Windows 2008 or Windows 7 machine, and copy the files to the OS Provisioning Server.

Prerequisites

- Verify that the Windows Automated Install Kit (WAIK) 2.0 is installed on the Windows machine on which you are creating the boot image.
- Verify that the Windows machine on which you are creating the image, which is usually the VCM Collector, can access the OS Provisioning Server on the network.
- On Windows 2008 machines, you run the command line options in this procedure as Administrator.

Procedure

1. On the OS Provisioning Server, copy `/opt/FastScale/deployment` to a directory on the Windows machines on which you are creating the boot image.

   For example, `c:\Program Files\osp`.

2. From the Windows command line, change the directory to the location where you copied the deployment files.

   For example, `c:\Program Files\osp\deployment`.

3. From the Windows command line, run `bin\osp --osphome="c:<Path to OSP files> --deploymenturl=<OS Provisioning Server Private IP Address> --waik=<Path to WAIK>"`.

Option	Description
`osphomee`	The path to the files copied from the OS Provisioning Server. For example, `c:\Program Files\osp\deployment`. If you run the command from the directory, you can use `--osphome=.`
`deploymenturl`	The OS Provisioning Server's Private Interface IP Address. The default configuration is 10.11.12.1.
`waik`	Path to the Windows AIK files. For example, `"c:\Program Files (x86)\Windows AIK"`.

4. When the preinstallation environment and boot configuration are created, copy the directories from the Windows AIK machine to the OS Provisioning Server.

From Windows AIK Machine	To OS Provisioning Server
`[path]\deployment\output\Boot`	`/FSboot/`
`[path]\deployment\output\windows\amd64\winpe.wim`	`/FSboot/windows/amd64/`
`[path]\deployment\output\windows\x86\winpe.wim`	`/FSboot/windows/x86/`

What to do next

Copy the VCM certificate to the OS Provisioning Server to ensure the successful installation of your Linux/ESX distributions. See "Copy the VCM Certificate to the OS Provisioning Server for Linux Provisioning" on page 27.

Copy the VCM Certificate to the OS Provisioning Server for Linux Provisioning

If you use the OS Provisioning Server to install Linux distributions, you must copy the VCM certificate file to the OS Provisioning Server to ensure the certificate is included with the Agent when OS Provisioning Server creates the configured session prior to provisioning.

Prerequistes

Ensure that you have access to the `VMware_VCM_Enterprise_Certificate_*.pem` file in the `\Program Files (x86)\VMware\VCM\CollectorData` folder on the VCM Collector.

Procedure

1. Copy the VCM certificate, `VMware_VCM_Enterprise_Certificate_*.pem`, to the OS Provisioning Server`/opt/FastScale/var/fsadmin/basic/` directory.

What to do next

Configure the secure Stunnel communications between the OS Provisioning Server and the VCM Collector. See "Configure OS Provisioning Server Integration with the VCM Collector" on page 28.

Configure OS Provisioning Server Integration with the VCM Collector

The integration between VCM and the OS Provisioning Server uses Stunnel to establish secure communication between and the SOAP services of the two components.

Prerequisites

- Ensure that all private keys are RSA keys.
- Ensure that certificates are created or obtained, and copied to the required locations using industry best practices.
- On the Collector, copy the certificate to `c:\Program Files (x86)\VMware\VCM\Tools\sTunnel\certs\vcm_stunnel_cert.pem`.
- On the Collector, copy the private key to `c:\Program Files (x86)\VMware\VCM\Tools\sTunnel\key\vcm_stunnel_pk.pem`.
- On the OS Provisioning Server, copy the certificate to `/opt/FastScale/var/certs/vcm_stunnel_cert.pem`.
- Verify that all directories where these keys and certificates are stored are secured.

Procedure

1. "Configure Stunnel on the OS Provisioning Server" on page 29.

   Stunnel is used to establish secure communication between VCM and the OS Provisioning Server SOAP services. On the OS Provisioning Server, copy the certificates to the locations specified in the `stunnel.conf` file and configure Stunnel to ensure that the connection on the OS Provisioning Server is operational.

2. "Configure Stunnel on the VCM Collector" on page 30.

   The VCM Collector installation process installs Stunnel files that are used to establish secure communication between VCM and the OS Provisioning Server SOAP services. Configure Stunnel to ensure that the connection on the Collector is operational.

3. "Confirm Stunnel Configuration" on page 32.

   Confirm that Stunnel communication between the OS Provisioning Server and the VCM Collector is configured and active before you provision target machines.

Configure Stunnel on the OS Provisioning Server

Stunnel is used to establish secure communication between VCM and the OS Provisioning Server SOAP services. On the OS Provisioning Server, copy the certificates to the locations specified in the `stunnel.conf` file and configure Stunnel to ensure that the connection on the OS Provisioning Server is operational.

Prerequisites

Review the VCM Stunnel certificate validation chain described in `/opt/FastScale/etc/stunnel.conf`.

Procedure

1. On the OS Provisioning Server, log in as `root`.
2. Place the VCM Stunnel certificate validation chain in `/opt/FastScale/var/certs`.

   All of the files in this directory are owned by `root` and have permissions of `-rw-r--r--`.

   The Stunnel configuration file on the OS Provisioning Server is located in `/opt/FastScale/etc/stunnel.conf`.

```
; stunnel configuration file for server proxy

; Some performance tunings

socket = l:TCP_NODELAY=1

socket = r:TCP_NODELAY=1

; debug = 7

cert = /opt/FastScale/var/certs/service.pem

key = /opt/FastScale/var/certs/private/service.key

; Either CAfile or CAPath, but not both, should be defined

; CAfile = /opt/FastScale/var/certs/ca-cert.pem

; Certificate Authority directory

; This is the directory in which stunnel will look for certificates
when using the verify.

; Note that the certificates in this directory should be named

; XXXXXXXX.0 where XXXXXXXX is the hash value of the DER encoded
subject of the

; cert (the first 4 bytes of the MD5 hash in least significant byte
order).

; The hash can be obtained with the command: openssl x509 -noout -in
cert.pem -hash

CApath = /opt/FastScale/var/certs

client = no

foreground = no

output = /opt/FastScale/logs/stunnel.log

pid = /opt/FastScale/logs/stunnel.pid

[fsmesgds]
```

```
accept = 40610
connect = localhost:21310
; Authentication stuff
verify = 3
[fsrepods]
accept = 40607
connect = 127.0.0.1:21307
; Authentication stuff
verify = 3
```

3. Run the `service FastScale restart` command to restart Stunnel.

What to do next

After you configure the Stunnel on the OS Provisioning Server, you must configure the Stunnel communication on the VCM Collector. See "Configure Stunnel on the VCM Collector" on page 30.

Configure Stunnel on the VCM Collector

The VCM Collector installation process installs Stunnel files that are used to establish secure communication between VCM and the OS Provisioning Server SOAP services. Configure Stunnel to ensure that the connection on the Collector is operational.

Prerequisites

- Secure the VCM Stunnel certificate and the VCM Stunnel private key according to your corporate best practices.
- Verify that the `[C:]\Program Files (x86)\VMware\VCM\Tools\sTunnel\certs\` directory exists on the Collector. If the directory does not exist, create it.
- Verify that the `[C:]\Program Files (x86)\VMware\VCM\Tools\sTunnel\key\` directory exists on the Collector. If the directory does not exist, create it.

Procedure

1. On the Collector, place the VCM Stunnel certificate in `[C:]\Program Files (x86)\VMware\VCM\Tools\sTunnel\certs\vcm_stunnel_cert.pem`.
2. Place the VCM Stunnel RSA private key in `[C:]\Program Files (x86)\VMware\VCM\Tools\sTunnel\key\vcm_stunnel_pk.pem`.
3. Place the OS Provisioning Server Stunnel CA certificate validation chain in the files and directory specified in the `stunnel.conf` file.

   The VCM Stunnel configuration file on the VCM application server is `[C:]\Program Files (x86)\VMware\VCM\Tools\stunnel.conf`.

   ```
   cert = C:\Program Files (x86)\VMware\VCM\Tools\sTunnel\certs\vcm_stunnel_
   cert.pem
   key = C:\Program Files (x86)\VMware\VCM\Tools\sTunnel\key\vcm_stunnel_pk.pem
   ;; Use stunnel in client mode
   client = yes
   ```

```
;; FIPS mode can be enabled as desired

fips = no

;; Some performance tunings

socket = l:TCP_NODELAY=1

socket = r:TCP_NODELAY=1

;; Either CAfile or CAPath, but not both, should be defined

;; CAfile contains the certificate chains needed to verify the certificates of
remote connections

;CAfile = C:\Program Files (x86)\VMware\VCM\Tools\sTunnel\certs\ca-cert.pem

;; CApath = directory

;; Certificate Authority directory

;; This is the directory in which stunnel will look for certificates when
using the verify.

;; Note that the certificates in this directory should be named

;; XXXXXXXX.0 where XXXXXXXX is the hash value of the DER encoded subject of
the

;; cert (the first 4 bytes of the MD5 hash in least significant byte order).

;; The hash can be obtained with the command: openssl x509 -noout -in cert.pem
-hash

CApath = C:\Program Files (x86)\VMware\VCM\Tools\sTunnel\certs

;; Some debugging stuff useful for troubleshooting

;debug = 7

;output = stunnel.log

;; verify = level

;; level 1 - verify peer certificate if present

;; level 2 - verify peer certificate

;; level 3 - verify peer with locally installed certificate

;; default - no verify

verify = 3

;; limit connections to certain ciphers

ciphers = AES128-SHA:DES-CBC3-SHA :@STRENGTH

;; asm_hostname_or_ip_address must be replaced with the correct value for the
OS Provisioning Server

[fsrepo]

accept = 127.0.0.1:21307

connect = asm_hostname_or_ip_address:40607
```

4. In the `stunnel.conf` file, update the local values.

Option	Description
`cert`	Update `C:\Program Files (x86)\VMware\VCM\Tools\sTunnel\certs\vcm_stunnel_cert.pem` with the installation location.
`key`	Update `C:\Program Files (x86)\VMware\VCM\Tools\sTunnel\key\vcm_stunnel_pk.pem` with the installation location.
`CAfile` or `CApath`	Use one of the options. ■ If using `CAfile`, update `C:\Program Files (x86)\VMware\VCM\Tools\sTunnel\certs\ca-cert.pem` with the installation location. ■ If using `CApath`, update `C:\Program Files (x86)\VMware\VCM\Tools\sTunnel\certs` with the installation location.
`accept`	Update to `127.0.0.1:21307`.
`connect`	Update `asm_hostname_or_ip_address:40607` to the host name or the IP address of the OS Provisioning Server.

5. Run the following commands from the Stunnel directory to register and start the Stunnel service.

```
cd c:\Program Files (x86)\VMware\VCM\Tools\sTunnel

stunnel –install

net start stunnel
```

What to do next

Verify that the communication between the OS Provisioning Server and the VCM Collector is properly configured. See "Confirm Stunnel Configuration" on page 32.

Confirm Stunnel Configuration

Confirm that Stunnel communication between the OS Provisioning Server and the VCM Collector is configured and active before you provision target machines.

Prerequisites

- Configure Stunnel on the OS Provisioning Server. See "Configure Stunnel on the OS Provisioning Server" on page 29.
- Configure Stunnel on the VCM Collector. See "Configure Stunnel on the VCM Collector" on page 30.

Procedure

1. On the Collector, start Internet Explorer and type `http://localhost:21307/` in the address field.

   If the connection is properly configured, the following message appears.

```
<?xml version="1.0" encoding="UTF-8" ?>

- <SOAP-ENV:Envelope xmlns:SOAP-
ENV="http://schemas.xmlsoap.org/soap/envelope/" xmlns:SOAP-
ENC="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:t="urn:types.fastscale.com"
xmlns:dos="urn:bobdos.fastscale.com" xmlns:wsns="http://tempuri.org/wsns.xsd"
xmlns:fst="urn:bob.fastscale.com">

- <SOAP-ENV:Body>

- <SOAP-ENV:Fault>

<faultcode>SOAP-ENV:Client</faultcode>

<faultstring>HTTP GET method not implemented</faultstring>

</SOAP-ENV:Fault>

</SOAP-ENV:Body>

</SOAP-ENV:Envelope>
```

   If the connection fails, the page displays `Web page not found`. You must review your Stunnel configuration files and make any necessary corrections.

What to do next

Import distributions into your OS Provisioning Server repository. See "Import Distributions into the OS Provisioning Server Repository" on page 33.

Import Distributions into the OS Provisioning Server Repository

To install operating system distributions on target machines, you must import the distributions into the OS Provisioning Server repository.

Supported operating systems are listed in the *VCM Hardware and Software Requirements Guide*.

Prerequisites

Confirm that you installed OS Provisioning Server and configured all the options. See "Install and Configure the OS Provisioning Server" on page 21.

Procedure

1. "Create Directories for Windows Distributions" on page 34.

   Some Windows operating system distribution files are issued on multiple disks. Because of the dependencies within the packages, you must create a single directory for multiple Windows operating system disks before you import Windows distributions.

2. "Import Windows Distributions" on page 34.

Windows distributions are the operating system installation files that you import into the OS Provisioning Server repository. After importing the distribution, you use VCM provisioning actions to install the operating system on target machines.

3. "Import Linux/ESX Distributions" on page 36.

   Linux/ESX distributions are the operating system installation files that you import into the OS Provisioning Server repository. After importing the distribution, use VCM provisioning actions to install the operating system on target machines. You can import standard and customized operating system distributions.

Create Directories for Windows Distributions

Some Windows operating system distribution files are issued on multiple disks. Because of the dependencies within the packages, you must create a single directory for multiple Windows operating system disks before you import Windows distributions.

Procedure

1. On the OS Provisioning Server, use the `mkdir -p /tmp/<directory name>` command to create a directory to contain the imported files from multiple source files.

   For example, `mkdir -p /tmp/Win2003-R2-SP2-Standard`.

2. Insert the first CD in the drive and run the `cp -R /media/cdrom/<source directory name> /tmp/<directory name>` command.

   For example, `cp -R /media/cdrom/Win2003-R2-SP2-Standard /tmp/Win2003-R2-SP2-Standard-Disk1`.

3. Replace the first CD with the second CD and run the `cp -R /media/cdrom/<source directory name> /tmp/<directory name>` command.

   For example, `cp -R /media/cdrom/Win2003-R2-SP2-Standard /tmp/Win2003-R2-SP2-Standard-Disk2`.

   When you import the second CD, do not replace any files if you are prompted during the copy operation.

What to do next

Import Windows distributions into your repository. See "Import Windows Distributions" on page 34.

Import Windows Distributions

Windows distributions are the operating system installation files that you import into the OS Provisioning Server repository. After importing the distribution, you use VCM provisioning actions to install the operating system on target machines.

You can import standard and customized ISO images. When you import a standard image, you type the required metadata. If the import process detects a custom image, you must select specific values for the platform, distribution, and build type.

When you mount the images, do not use `-t iso9660`. If you use `-t iso9660`, some auto-mounted media will not import. If the import process reports a fingerprint error message, you must unmount the directory and manually mount it using the `-t udf` rather than the `-t iso9660` option.

Prerequisites

- Verify that the distributions you are importing do not include spaces in the filenames. Before you import, remove the spaces or replace them with underscores.
- Confirm that the current OS Provisioning Server IP address is correct for your production environment. You cannot change the OS Provisioning Server IP address at a later time. If the initial IP address of the OS Provisioning Server after install is not the address you intend for it to have when it is put into production, you must change its address, and change related DHCP and TFTP configurations, before you import any OS distributions. If you change the OS Provisioning Server IP address after you imported the distributions, you must re-import the distributions with the new address. You must also recreate the Windows boot image with the new IP address.
- Determine whether you are importing a single ISO image or multiple images from a directory. The `basicimport` command uses a `-i` option to specify an ISO file and a `-d` option to specify the directory. See "Using the basicimport Command Options" on page 38.
- If you are importing multidistribution `.iso` files, create directories and copy the files to the directories. See "Create Directories for Windows Distributions" on page 34.

Procedure

1. On the OS Provisioning Server, log in as `vcmuser`.
2. Mount the ISO by attaching to the media image or mounting the image.

   For Windows 2008 and Windows 7, use `-t udf` mount type and do not include any spaces in the path.

   For all other Windows operating systems, use loopback. For example, `$ sudo mount -o loop /<iso_file.iso> /<mount point>`.
3. Run the `sudo basicimport -d /mnt/<directory name> -l <OS Provisioning Server private IP address or provisioning network IP address>` command.

   For example, `sudo basicimport -d /mnt/Win2k3SE-R2-SP2-i386 -l 10.11.12.1`.

   If you created a `/tmp/` directory for a multi-CD distribution, include the path. For example, `/tmp/<directory name>`, or `/tmp/Win2003-R2-SP2-Standard`.

   For subsequent imports, you can run the command without the `-l` option.
4. Type the Family Name.

   For example, `Windows`. You must provide a unique family name to import different operating systems in the same family. No other family can exist with the same combination of name, version, and architecture values.
5. Type the Family Version.

   For example, `2008R2`.
6. Type the Family Architecture.

   For example, either `i386` or `x86_64`.
7. Type the Provenance.

   For example, `CD`, `hotfix`, or `SP`.
8. For Windows 2008 R2, Windows 7, and Windows 2003 only, type the Build Type.

   For example, either `volume` or `retail`.

If you importing a standard ISO, the distribution is imported. If the ISO is customized, you must provide additional information about the distribution that is used when installing the operating system.

9. In the OS platform list, select `1. Microsoft Windows`.
10. In the OS distributions list, select the number that most closely corresponds to the operating system you are importing.

    ```
    1. Microsoft Windows Server 2008 R2
    2. Microsoft Windows Server 2008 SP2
    3. Microsoft Windows Server 2008 SP1
    4. Microsoft Windows 7
    5. Microsoft Windows 2003, Enterprise Edition R2 SP2
    6. Microsoft Windows 2003, Standard Edition R2 SP2
    ```

    If you select the incorrect distribution, you can import the distributions, but you cannot install it.
11. Type the Build Type, either `retail` or `volume`.

    The distribution is imported.

What to do next

Import Linux/ESX distributions into the OS Provisioning Server repository. See "Import Linux/ESX Distributions" on page 36

Import Linux/ESX Distributions

Linux/ESX distributions are the operating system installation files that you import into the OS Provisioning Server repository. After importing the distribution, use VCM provisioning actions to install the operating system on target machines. You can import standard and customized operating system distributions.

You can import standard and customized ISO images. When you import a standard image, you type the required metadata during the import process. If the import process detects a custom image, you must select specific values for the platform and distribution.

Use this procedure to import Linux or ESX distributions. For SUSE distributions that are issued on multiple DVDs, you use only the first disk and import the distribution using this procedure.

Prerequisites

- Verify that the distributions you are importing do not include spaces in the filenames. Before you import, remove the spaces or replace them with underscores.
- Confirm that the current OS Provisioning Server IP address is correct for your production environment. You cannot change the OS Provisioning Server IP address at a later time. If the initial IP address of the OS Provisioning Server after install is not the address you intend for it to have when it is put into production, you must change its address, and change related DHCP and TFTP configurations, before you import any OS distributions. If you change the OS Provisioning Server IP address after you imported the distributions, you must re-import the distributions with the new address.
- Determine whether you are importing a single ISO image or multiple images from a directory. The `basicimport` command uses a `-i` option to specify an ISO file and a `-d` option to specify the directory. See "Using the basicimport Command Options" on page 38.

Procedure

1. On the OS Provisioning Server, log in as `vcmuser`.
2. Mount the ISO by attaching to the media image or mounting the image.

   For all UNIX, Linux, or ESX operating systems, use loopback. For example, `$ sudo mount -o loop <iso_file.iso> /<mount point>`.
3. Run the `sudo basicimport -i <distribution name>.iso -l <OS Provisioning Server private IP address or provisioning network IP address>` command.

   For example, `sudo basicimport -i ESX-4.0.0-update01-208167.iso -l 10.11.12.1`.

   For subsequent imports, you can run the command without the `-l` option.
4. Type the Family Name.

   For example, `ESX` or `Linux`. You must provide a unique family name to import different operating systems in the same family. No other family can exist with the same combination of name, version, and architecture values.
5. Type the Family Version.

   For example, `4.0ul`.
6. Type the Family Architecture.

   For example, either `i386` or `x86_64`.
7. Type the Provenance.

   For example, `CD`, `hotfix`, or `SP`.

   If you importing a standard ISO, The distribution is imported.. If the ISO is customized, you must provide additional information about the distribution that is used when installing the operating system.
8. In the OS platform list, select the number corresponding to your distribution platform, either `2. Linux` or `3. VMware Hypervisor Platform`.
9. In the OS distributions list, select the number that most closely corresponds to the operating system you are importing.

Linux	VMware Hypervisor Platform
1. RedHat Enterprise Linux 6	1. ESXi 5.0
2. RedHat Enterprise Linux 5.6	2. ESXi 4.1 Update1
3. RedHat Enterprise Linux 5.5	3. ESXi 4.1
4. RedHat Enterprise Linux 5.4	4. ESX 4.1 Update1
5. RedHat Enterprise Linux 5.2	5. ESX 4.1
6. RedHat Enterprise Linux 5.0	6. ESX 4.0 Update2
7. Suse Linux Enterprise 11.1	7. ESX 4.0 Update1
8. Suse Linux Enterprise 10.3	

   If you select the incorrect distribution, you can import the distributions, but you cannot install it.

   The distribution is imported.

What to do next

Using VCM, you install distributions on target machines. See "Getting Started with Operating System Provisioning" on page 199.

Using the basicimport Command Options

You use the `basicimport` command-line options to import UNIX, Linux, ESX, or Windows distributions into the OS Provisioning Server repository.

Table 3–1. basicimport Command Options

Option	Description
`-h`	Help. Displays and describes the `basicimport` options.
`-d`	Directory. Path to the media source directory. This option is required when you import OS distributions issued on more than one media item, such as multiple DVDs.
`-i`	ISO file. Path and image name for the distribution. Used with importing distributions issued on one media source, such as a Red Hat distribution on a single DVD.
`-l`	Deployment IP address of the OS Provisioning Server.
`-n`	Family name. For example, `ESX` or `Windows`.
`-V`	Family version. For example, `4.0u1` or `2008r2sp2`.
`-a`	Family Architecture. For example, `i386` or `x86_64`.
`-p`	Provenance. Distribution source. For example, `CD`, `hotfix`, or `SP`.
`-t`	ISO build type. For example, `retail` or `volume`. Applies only to Windows Server 2008 R2, Windows 7, and Windows Server 2003.

Working with Custom Linux ISO Distributions

The OS Provisioning Server in VCM allows you to import custom Red Hat and SUSE ISO images into the repository and then to install the custom distributions on target machines.

To support standard and custom ISO images, OS Provisioning Server includes required package lists for each supported ISO. If your custom ISO is missing any of the packages specified in the list, or is missing any of the dependencies specified by the required packages, you can import the ISO into the repository, but the installation of a distribution lacking a required or dependency package may fail.

To provide you with the flexibility to use OS provisioning to install your custom distribution, you have the two options.

- Add the missing required packages back into the ISO and re-import it into the repository. Run the Provision wizard again to create a new configured session with the updated distribution. The installation of the distribution on the target machines will proceed without an error and the required list remains as it was provided in the OS Provisioning Server.
- Modify the required package list by removing the package names from the list. The installation of the distribution on the target machines will proceed without an error unless there are missing dependency packages.

The required package lists, whether you are using them for reference, as in the first option, or are modifying them, as in the second option, are located on the OS Provisioning Server.

- **Red Hat:** `/FSboot/repository/linux/<RHEL version>`.

  For example, `/FSboot/repository/linux/RHEL6.0server-x86_64/packages`
- **SLES 10.3:** `/opt/FastScale/var/fsadmin/jobs/SLES10.0_sp3.basic.php`
- **SLES 11.1:** `/opt/FastScale/var/fsadmin/jobs/SLES11.0_sp1.basic.php`

For error messages due to missing packages, see the *VCM Troubleshooting Guide*.

Upgrade the OS Provisioning Server to 5.4.1

You cannot directly upgrade from OS Provisioning Server 5.4 to 5.4.1. Nor is OS Provisioning Server 5.4 compatible with VCM 5.4.1. You must install the new 5.4.1 OS Provisioning Server components, configure the server, and import the operating system ISO files into the new database structure.

Before Upgrading the OS Provisioning Server

Review the upgrade constraints.

- If the target machines in your current Provisionable Machines and Provisioned Machines data grids in VCM are machines you intend to manage with VCM, complete the provisioning process, license, install the Agent, and collect data from the target machines. This action ensures that the machines continue as managed machines. All provisioning history and the ability to reprovision the managed machines from the Provisioned Machines data grid is no long available after you upgrade.
- Ensure that there are no outstanding provisioning actions. The Provisionable Machines data grid should not include any target machines that must be installed before you upgrade. Click **Administration** and select **Machines Manager > OS Provisioning > Provisionable Machines**.

Upgrading the OS Provisioning Server

The OS Provisioning Server includes new components and a new database structure. You cannot use any part of the 5.4 OS Provisioning Server. You must uninstall your existing OS Provisioning Server server and configure the system as specified in the *VCM Hardware and Software Requirements Guide*, then install and configure the new OS Provisioning Server. See "Installing, Configuring, and Upgrading the OS Provisioning Server and Components" on page 21.

You must also import your distributions into the new database structure. See "Import Distributions into the OS Provisioning Server Repository" on page 33.

In VCM, after you install, configure, and import the distributions, you must collect the OS distributions from the new OS Provisioning Server before you can begin provisioning target machines. See "Getting Started with Operating System Provisioning" on page 199.

After Upgrading the OS Provisioning Server

All provisioned machines that were licensed, on which the Agent was installed, and from which data was collected are fully managed machines in VCM. They are displayed in VCM based on the installed operating system. However, they are not longer displayed in the Provisioned Machines data grid and they are not available for reprovisioning using the Re-provision wizard.

Managing the OS Provisioning Server System Logs

The OS Provisioning Server log files are located in the `/opt/FastScale/logs` and `/var/log` directories. You must monitor the space used and truncate the files if they begin to consume more disk space on the server than you have space to store.

Table 3–2. Log File Locations

Directory	File Name	Description
`/opt/FastScale/logs`	`fsadmin.err`	Messages from the Apache Web server.
	`fsadmin.log`	Lists internal commands from the Apache Web server.
	`FSjobd.log`	Messages generated during the job build process.
	`FSmesgd.log`	Messages generated by the message daemon.
	`FSnetfs.log`	Messages from the FSnetfs service.
	`FSrepod.log`	Messages generated by the repository database server.
	`php.log`	Messages from the php interpreter used by the Web server and the jobs build program.
	`stunnel.log`	Messages generated by Stunnel services for Stunnel services communication between the OS Provisioning Server and VCM.
`/var/log`	`messages`	Messages from dhcpd and tftpd services generated during hardware discovery and operating system deployment to target machines.

ospctrl Command Options

Use the `ospctrl` command-line options to configure your TFTP and Apache services with the OS provisioning private IP address and to back up and restore the OS Provisioning Server repository and distribution files.

Table 3–3. ospctrl Command Options

Option	Description
`--help`	Displays and describes the `ospctrl` options.
`--showconfig`	Displays the current state of the TFTP and Apache servers, including the configured private IP address.
`--configure --privateip <IPAddress>`	Configures the TFTP server and the Apache server with the private provisioning network IP address.
`--deconfigure`	Resets the TFTP server and the Apache server to the default values.
`--backup --dirpath=/<path to backup directory>`	Backs up the repository and the OS distributions to the specified `--dirpath` location.

Option	Description
`--restore --dirpath=/<path to backup directory>`	Restores the repository and the OS distributions from the specified `--dirpath` backup location.

Upgrading or Migrating VCM 4

You can upgrade or migrate your existing VCM environment to VCM 5.4.1, which supports 64-bit environments that include 64-bit hardware, 64-bit Windows Server 2008 R2 and SP1, and SQL Server 2008 R2 and SP1.

You can use Installation Manager to upgrade from VMware VCM 5.3, EMC Ionix SCM 5.0 or greater, or Configuresoft ECM 4.11.1 or greater to VCM 5.4.1.

When you perform a new installation or a migration, you must have the previous license file available and specify the path to the license file during the installation. Installation Manager uses the license file to activate the components that you purchased. If you do not have the license file from VCM 4.11.1 or later, contact VMware Technical Support.

You must determine whether your VCM environment requires an upgrade or a migration. The prerequisites and steps differ depending on whether you perform an upgrade or a migration of VCM.

Upgrades

An upgrade to VCM 5.4.1 uses an existing VCM Collector installation. You upgrade the operating system, SQL Server, and VCM to the versions associated with VCM 5.4.1.

VCM 5.4.1 supports the following upgrade paths.

- Upgrade from VCM 5.4, which is a 64-bit single-server installation. Updates to Windows Server 2008 R2 or SQL Server 2008 R2 are not required.
- Upgrade from a 64-bit single-server installation that includes VMware VCM 5.3 or later, EMC Ionix SCM 5.0 or later, or Configuresoft ECM 4.11.1 or later. You must upgrade to Windows Server 2008 R2 and SQL Server 2008 R2 are required.

Migrations

A migration to VCM 5.4.1 requires you to prepare new hardware and software for your environment. VCM 5.4.1 supports the following migration paths.

- Migrate from a 32-bit or 64-bit environment that includes VCM, SCM, or ECM.
- Migrate a split installation of VCM to a single-server installation of VCM 5.4.1.

You must update your hardware to 64-bit. Update the operating system to the 64-bit Windows Server 2008 R2 operating system, update to SQL Server 2008 R2, and update SQL Server Reporting Services. Then you can migrate your existing VCM, SCM, or ECM installation to your new VCM 5.4.1 environment.

What to do next

Understand the prerequisites to prepare and migrate your VCM environment to VCM 5.4.1. See "Prerequisites to Migrate VCM" on page 44.

Prerequisites to Migrate VCM

Before you migrate your existing VCM environment to VCM 5.4.1, you must perform several prerequisites. If you have any questions about the migration procedures, contact VMware Technical Support before you begin the migration.

- Review and understand the migration scenarios. See "Upgrading or Migrating VCM" on page 43.
- Verify that your existing VCM installation is functional.
- Verify that your VCM Collector meets all of the hardware and software requirements for a 64-bit environment. For a complete list of requirements, see the *VCM Hardware and Software Requirements Guide*.
- Verify that your Configuration Manager version to migrate is either VMware VCM 5.3, EMC Ionix SCM 5.0 or later, or Configuresoft ECM 4.11.1 or later.
- If your VCM Collector is installed on a 32-bit Windows machine, understand the system requirements for VCM 5.4.1. See the *VCM Hardware and Software Requirements Guide*.
- Verify that an existing 32-bit environment includes SQL Server 2005 and SP3.
- Verify that an existing 64-bit environment includes 64-bit SQL Server 2005 and SP2, 32-bit SQL Server Reporting Services (SSRS), and SSRS SP3. The 32-bit version of SSRS is required in 64-bit environments of VCM 5.3 and earlier.
- Verify that your environment includes the required versions of the Microsoft .NET Framework. See the *VCM Hardware and Software Requirements Guide*.
- Back up your databases. See "Back Up Your Databases" on page 45.
- Back up the `CMFILES$` share. See "Back up Your Files" on page 45.
- Back up any files that you used to customize your Collector.
- Back up any reports that you exported to a non-default location.
- Back up your certificates. See "Export and Back up Your Certificates" on page 45.
- Verify that all jobs have finished running.
- Verify that no jobs are scheduled to begin during the migration process. The migration process stops the `SQLAgent` service, which prevents jobs from starting.
- Verify that all users have logged off of VCM.
- Ensure that users will not attempt to access VCM until you finish the migration process.
- Run Foundation Checker as a standalone utility on your VCM Collector to ensure that it is ready for the installation of VCM 5.4.1. See the *VCM Hardware and Software Requirements Guide*.
- Obtain the installation package from the Download VMware vCenter Configuration Manager Web site or the VCM 5.4.1 CD. You will install VCM as a final step in the migration process.
- Download the VCM SQL Migration Helper Tool from the Download VMware vCenter Configuration Manager Web site to help you reconfigure scheduled jobs and membership logins in your new environment.

Back Up Your Databases

Before you migrate an existing VCM environment to VCM 5.4.1, back up your databases to avoid any potential loss of data.

Depending on your existing version of VCM, SCM, or ECM, or the custom names that you chose during installation, the database names differ.

Table 4–1. Back Up Your Databases Before You Start the Migration Process

Version to Migrate	Back up these databases
VMware VCM	`CSI_Domain`, `VCM`, `VCM_Coll`, `VCM_UNIX`, `ReportServer`, `master`, and `msdb`
EMC Ionix SCM	`CSI_Domain`, `SCM`, `SCM_Coll`, `SCM_UNIX`, `ReportServer`, `master`, and `msdb`
Configuresoft ECM (versions 4.11.1 to 5.0)	`CSI_Domain`, `ECM`, `ECM_Coll`, `ECM_UNIX`, `ReportServer`, `master`, and `msdb`

Back up Your Files

Before you migrate an existing VCM environment to VCM 5.4.1, back up your files to avoid any potential loss of data.

1. Back up the entire content of the `CMFILES$` share.
   - For **64-bit systems:** `C:\Program Files (x86)\VMware\VCM\WebConsole\L1033\Files\`, or in the path relative to where you installed the software.
   - For **32-bit systems:** `C:\Program Files\VMware\VCM\WebConsole\L1033\Files\`, or in the path relative to where you installed the software.

   If your VCM Collector is part of an installation of EMC Ionix SCM or Configuresoft ECM, the path differs.
2. Back up any files used to customize your Collector.
3. Back up any reports that exist in a location other than the default location.

Export and Back up Your Certificates

Export and back up your VCM Collector and Enterprise certificates.

Procedure

1. On your VCM Collector, click **Start > Run**. Type `mmc.exe`.
2. In the Console window, click **File** and select **Add/Remote Snap-in**.
3. In the Add/Remote Snap-in dialog box, click the **Standalone** tab and click **Add**.
4. In the Add Standalone Snap-in dialog box, select **Certificates** and click **Add**.
5. In the Certificates snap-in dialog box, select **Computer account** and click **Next**.
6. In the Select Computer dialog box, select **Local Computer** and click **Finish**.

   The Certificates (Local Computer) is added to the list of certificates on the Standalone tab.
7. Click **Close** to close the Add Standalone Snap-in dialog box.

8. In the Add/Remove Snap-in dialog box, click **OK**.

   The Certificates (Local Computer) is added to the Console Root.

9. Expand **Console Root** and select **Certificates > Personal > Certificates**.
10. In the right pane, right-click the Collector certificate and select **All Tasks > Export**.
11. On the Certificate Export Wizard Welcome page, click **Next**.
12. On the Export Private Key page, select **No** and click **Next**.
13. On the Export File Format page, select **DER encoded binary** and click **Next**.
14. On the File to Export page, type the path and name or click **Browse** to specify the location of the file on the Collector or shared location, and click **Next**.
15. On the Completing the Certificate Export Wizard page, click **Finish**.

    The `.cer` file is now in the location that you specified in the export process.

Migrating VCM

To prepare your environment for VCM 5.4.1, you can choose to migrate only your databases, replace an existing 32-bit environment, migrate an existing 32-bit or 64-bit environment, or migrate a split installation.

Prerequisites

Before you migrate any part of your existing VCM environment to VCM 5.4.1, you must perform the prerequisites. See "Prerequisites to Migrate VCM" on page 44.

Procedure

- "Migrate Only Your Database " on page 46

  Migrate only your VCM database from version 4.11.1 or later.

- "Replace Your Existing 32-Bit Environment with a Supported 64-bit Environment" on page 47

  Replace an existing 32-bit environment of VMware VCM, EMC Ionix SCM, or Configureoft ECM.

- "Migrate a 32-bit Environment Running VCM 5.3 or Earlier to VCM 5.4.1" on page 48

  Migrate an existing 32-bit Collector to VCM 5.4.1. A migration to VCM 5.4.1 requires you to prepare new hardware and software for your environment and install the required software components.

- "Migrate a 64-bit Environment Running VCM 5.3 or Earlier to VCM 5.4.1" on page 49

  Migrate an existing 64-bit Collector to VCM 5.4.1. A migration to VCM 5.4.1 requires you to prepare new software for your environment and install the required software components.

- "Migrate a Split Installation of VCM 5.3 or Earlier to a Single-Server Installation" on page 51

  Migrate an existing split installation to a single-server installation for VCM 5.4.1. A split installation configuration placed the VCM Collector database on the Collector machine and the other VCM databases on a separate server machine.

Migrate Only Your Database

Migrate only your VCM database from version 4.11.1 or later.

Prerequisites

- Understand the scenarios to migrate your VCM environment to VCM 5.4.1. See "Upgrading or Migrating VCM" on page 43.
- Understand the prerequisites to migrate your VCM environment to VCM 5.4.1. See "Prerequisites to Migrate VCM" on page 44.
- Understand how to attach a SQL server database in SQL Server Management Studio. See the Microsoft MSDN Library.
- Install SQL Server 2008 R2 on the Windows machine that will host the VCM database.

Procedure

1. Move the VCM database to a prepared machine that has 64-bit SQL Server 2008 R2 installed.
2. On the prepared machine, start SQL Server Management Studio.
3. Attach the database to SQL Server 2008 R2.
4. Confirm that the `sa` account or the VCM service account is the owner of the newly attached database.

What to do next

Install VCM 5.4.1. See "Installing VCM" on page 19.

Replace Your Existing 32-Bit Environment with a Supported 64-bit Environment

Replace an existing 32-bit environment of VMware VCM, EMC Ionix SCM, or Configureoft ECM.

Previous versions of VMware VCM, EMC Ionix SCM, and Configureoft ECM support older versions of SQL Server. Your 32-bit environment must include specific software components before you replace your 32-bit environment and upgrade to VCM 5.4.1.

Prerequisites

- Understand the scenarios to migrate your VCM environment to VCM 5.4.1. See "Upgrading or Migrating VCM" on page 43
- Perform the prerequisites to migrate your VCM environment to VCM 5.4.1. See "Prerequisites to Migrate VCM" on page 44.
- Ensure that your environment is functional before you replace it and upgrade to VCM 5.4.1.

Procedure

1. Verify that your existing 32-bit installation of Configuration Manager is version 4.11.1 or later.
2. If your existing 32-bit installation is not 4.11.1 or later, use the appropriate installation packages and documentation to upgrade your existing installation to version 4.11.1 or later.
3. Verify that your 32-bit environment includes the following software components.

   If these software components are not installed, install them in the order listed.

   a. SQL Server 2005

   b. SQL Server Reporting Services, 32-bit version

   c. SQL Server 2005 SP3

4. Replace your 32-bit Windows Collector machine with a 64-bit machine.
5. Install the 64-bit Windows Server 2008 R2 operating system on the 64-bit Windows Collector machine.
6. Upgrade VCM to VCM 5.4.1.

What to do next

- Configure the SQL Server settings to tune your VCM database in SQL Server Management Studio, including the VCM database file growth and database recovery. See "Maintaining VCM After Installation" on page 65.
- Log in to VCM.

Migrate a 32-bit Environment Running VCM 5.3 or Earlier to VCM 5.4.1

Migrate an existing 32-bit Collector to VCM 5.4.1. A migration to VCM 5.4.1 requires you to prepare new hardware and software for your environment and install the required software components.

CAUTION Before you begin the migration, to avoid any potential loss of data you must perform the prerequisite steps to back up your files, including the VCM databases, the `CMFILES$` share, any files used to customize the VCM Collector, reports that are exported to a non-default location, and your certificates.

Prerequisites

- Understand the scenarios to migrate your VCM environment to VCM 5.4.1. See "Upgrading or Migrating VCM" on page 43.
- Perform the prerequisites to migrate your VCM environment to VCM 5.4.1. See "Prerequisites to Migrate VCM" on page 44.
- Understand how to detach and attach a SQL server database in SQL Server Management Studio. See the online Microsoft MSDN Library.
- Understand how to use the `sp_changedbowner` stored procedure. See SQL Server 2008 R2 Books Online in the online Microsoft MSDN Library.
- Determine if your 64-bit Collector machine is configured for Secure Sockets Layer (SSL).
- Use the SQL Migration Helper Tool to create a script for scheduled jobs on your 32-bit Collector. You can then import the scheduled jobs into your 64-bit Collector.
- Use the SQL Migration Helper Tool to create a script that contains your existing login and role membership information on your 32-bit Collector. You can then import your logins and roles into your 64-bit Collector.
- Locate the VCM 5.4.1 installation package on the Download VMware vCenter Configuration Manager Web site or obtain the VCM 5.4.1 CD.
- Ensure that your environment is functional before you migrate VCM 5.3 or earlier to VCM 5.4.1.

Procedure

1. On your 64-bit VCM Collector Windows machine, install Windows Server 2008 R2.
2. Install SQL Server 2008 R2 on your 64-bit VCM Collector.
3. Stop the VCM Collector service and the VCM Patch Management service.
4. On your 32-bit VCM Collector, use SQL Server Management Studio Object Explorer to detach the VCM databases.

5. On your 64-bit Collector, use SQL Server Management Studio Object Explorer to attach or restore the VCM databases to SQL Server 2008 R2.
6. On your 64-bit Collector, verify that the owner for the restored or attached databases is set to the `sa` account or the VCM service account.

   You can use the built-in `sp_changedbowner` stored procedure to change the ownership of the databases.
7. Start the VCM 5.4.1 installation and select the **Install** option.

   CAUTION When you begin the VCM installation, do not select the **Repair** option unless you are directed by VMware Technical Support. The repair process requires access to your original installation media to check for and replace missing files and settings.

   When the installation begins, VCM Foundation Checker gathers information about the Collector machine. If errors occur, you must resolve them before you can proceed.
8. Make sure that you select all of the components for installation.

   If a component cannot be upgraded due to an invalid upgrade or an incomplete copy of the install image, Installation Manager clears the check box and displays a message.
9. If you plan to upgrade VCM Remote and continue to use older Agents, use the same name for the new Remote virtual directory as used in your previous installation.

   If you change the Remote virtual directory name, you must update all corresponding Agents to use the new virtual directory.
10. Select your existing databases to migrate them to VCM 5.4.1.

    If Installation Manager requests that you create a new database, select the previous wizard page and verify that your existing database, which you attached, is selected.
11. Do not select SSL unless your machine is already configured for SSL.
12. After the upgrade is finished, copy the content of `WebConsole\L1033\Files` from your 32-bit Collector to your 64-bit Collector.

    Any existing remote commands, discovery files, and imported template files in this directory are available on the 64-bit Collector.
13. On your 64-bit Collector, run your script to import your VCM scheduled jobs.
14. On your 64-bit Collector, run your script to import your VCM membership logins.
15. Re-import any custom SQL Server Reporting Service Report Definition Language (RDL) files.

What to do next

- Configure the SQL Server settings to tune your VCM database in SQL Server Management Studio, including the VCM database file growth and database recovery. See "Maintaining VCM After Installation" on page 65.
- Log in to VCM.

Migrate a 64-bit Environment Running VCM 5.3 or Earlier to VCM 5.4.1

Migrate an existing 64-bit Collector to VCM 5.4.1. A migration to VCM 5.4.1 requires you to prepare new software for your environment and install the required software components.

Use this method as part of the VCM 5.4.1 installation process to replace the VCM hardware, change the operating system version, or install a new operating system. You install a new environment, copy the VCM databases and other components, and then install VCM 5.4.1. During the installation, you select the existing VCM database.

CAUTION Before you begin the migration, to avoid any potential loss of data you must perform the prerequisite steps to back up your files, including the VCM databases, the `CMFILES$` share, any files used to customize the VCM Collector, reports that are exported to a non-default location, and your certificates.

Prerequisites

- Understand the scenarios to migrate your VCM environment to VCM 5.4.1. See "Upgrading or Migrating VCM" on page 43.
- Perform the prerequisites to migrate your VCM environment to VCM 5.4.1. See "Prerequisites to Migrate VCM" on page 44.
- Understand how to detach and attach a SQL server database in SQL Server Management Studio. See the online Microsoft MSDN Library.
- Understand how to use the `sp_changedbowner` stored procedure. See SQL Server 2008 R2 Books Online in the online Microsoft MSDN Library.
- Determine if your 64-bit Collector machine is configured for Secure Sockets Layer (SSL).
- Use the SQL Migration Helper Tool to create a script for scheduled jobs on your existing 64-bit Collector. You can then import the scheduled jobs into your new 64-bit Collector.
- Use the SQL Migration Helper Tool to create a script that contains your existing login and role membership information on your existing 64-bit Collector. You can then import your logins and roles into your new 64-bit Collector.
- Locate the VCM 5.4.1 installation package on the Download VMware vCenter Configuration Manager Web site or obtain the VCM 5.4.1 CD.
- Ensure that your environment is functional before you migrate VCM 5.3 or earlier to VCM 5.4.1.

Procedure

1. On your 64-bit VCM Collector Windows machine, install Windows Server 2008 R2.
2. Install SQL Server 2008 R2 on your 64-bit VCM Collector.
3. Stop the VCM Collector service and the VCM Patch Management service.
4. On your existing 64-bit VCM Collector, use SQL Server Management Studio Object Explorer to detach the VCM databases.
5. On your new 64-bit Collector, use SQL Server Management Studio Object Explorer to attach or restore the VCM databases to SQL Server 2008 R2.
6. On your 64-bit Collector, verify that the owner for the restored or attached databases is set to the `sa` account or the VCM service account.

   You can use the built-in `sp_changedbowner` stored procedure to change the ownership of the databases.
7. Start the VCM 5.4.1 installation and select the **Install** option.

CAUTION When you begin the VCM installation, do not select the **Repair** option unless you are directed by VMware Technical Support. The repair process requires access to your original installation media to check for and replace missing files and settings.

When the installation begins, VCM Foundation Checker gathers information about the Collector machine. If errors occur, you must resolve them before you can proceed.

8. Make sure that you select all of the components for installation.

   If a component cannot be upgraded due to an invalid upgrade or an incomplete copy of the install image, Installation Manager clears the check box and displays a message.

9. If you plan to upgrade VCM Remote and continue to use older Agents, use the same name for the new Remote virtual directory as used in your previous installation.

   If you change the Remote virtual directory name, you must update all corresponding Agents to use the new virtual directory.

10. Select your existing databases to migrate them to VCM 5.4.1.

    If Installation Manager requests that you create a new database, select the previous wizard page and verify that your existing database, which you attached, is selected.

11. Do not select SSL unless your machine is already configured for SSL.

12. After the upgrade is finished, copy the content of `WebConsole\L1033\Files` from your existing 64-bit Collector to your new 64-bit Collector.

    Any existing remote commands, discovery files, and imported template files in this directory are available on the 64-bit Collector.

13. On your 64-bit Collector, run your script to import your VCM scheduled jobs.

14. On your 64-bit Collector, run your script to import your VCM membership logins.

15. Re-import any custom SQL Server Reporting Service Report Definition Language (RDL) files.

What to do next

- Configure the SQL Server settings to tune your VCM database in SQL Server Management Studio, including the VCM database file growth and database recovery. See "Maintaining VCM After Installation" on page 65.
- Log in to VCM.

Migrate a Split Installation of VCM 5.3 or Earlier to a Single-Server Installation

Migrate an existing split installation to a single-server installation for VCM 5.4.1. A split installation configuration placed the VCM Collector database on the Collector machine and the other VCM databases on a separate server machine.

In a previous split installation, the VCM databases are installed as follows.

- **Collector machine:** Hosts the `VCM_Coll` database only.
- **Database Server machine:** Hosts the `VCM`, `VCM_UNIX`, `ReportServer`, `master`, and `msdb` databases.

The 64-bit single-server configuration used for VCM 5.4.1 installs all of the VCM databases on the Collector machine.

CAUTION Before you begin the migration, to avoid any potential loss of data you must perform the prerequisite steps to back up your files, including the VCM databases, the `CMFILES$` share, any files used to customize the VCM Collector, reports that are exported to a non-default location, and your certificates.

Prerequisites

- Understand the scenarios to migrate your VCM environment to VCM 5.4.1. See "Upgrading or Migrating VCM" on page 43.
- Perform the prerequisites to migrate your VCM environment to VCM 5.4.1. See "Prerequisites to Migrate VCM" on page 44.
- Understand how to detach and attach a SQL server database in SQL Server Management Studio. See the online Microsoft MSDN Library.
- Understand how to use the `sp_changedbowner` stored procedure. See SQL Server 2008 R2 Books Online in the online Microsoft MSDN Library.
- Determine if your 64-bit Collector machine is configured for Secure Sockets Layer (SSL).
- Use the SQL Migration Helper Tool to create a script for scheduled jobs on your 32-bit Collector. You can then import the scheduled jobs into your 64-bit Collector.
- Use the SQL Migration Helper Tool to create a script that contains your existing login and role membership information on your 32-bit Collector. You can then import your logins and roles into your 64-bit Collector.
- Locate the VCM 5.4.1 installation package on the Download VMware vCenter Configuration Manager Web site or obtain the VCM 5.4.1 CD.
- Ensure that your environment is functional before you migrate VCM 5.3 or earlier to VCM 5.4.1.

Procedure

1. On your 64-bit VCM Collector Windows machine, install Windows Server 2008 R2.
2. Install SQL Server 2008 R2 on your 64-bit VCM Collector.
3. Stop the VCM Collector service and the VCM Patch Management service.
4. On your 32-bit VCM Collector, use SQL Server Management Studio Object Explorer to detach the VCM databases.
5. On your 64-bit Collector, use SQL Server Management Studio Object Explorer to attach or restore the VCM databases to SQL Server 2008 R2.

   For a split installation, you must attach the databases from the Database Server to SQL Server 2008 R2.
6. On your 64-bit Collector, verify that the owner for the restored or attached databases is set to the `sa` account or the VCM service account.

   You can use the built-in `sp_changedbowner` stored procedure to change the ownership of the databases.
7. Start the VCM 5.4.1 installation and select the **Install** option.

   CAUTION When you begin the VCM installation, do not select the **Repair** option unless you are directed by VMware Technical Support. The repair process requires access to your original installation media to check for and replace missing files and settings.

When the installation begins, VCM Foundation Checker gathers information about the Collector machine. If errors occur, you must resolve them before you can proceed.

8. Make sure that you select all of the components for installation.

   If a component cannot be upgraded due to an invalid upgrade or an incomplete copy of the install image, Installation Manager clears the check box and displays a message.

9. If you plan to upgrade VCM Remote and continue to use older Agents, use the same name for the new Remote virtual directory as used in your previous installation.

   If you change the Remote virtual directory name, you must update all corresponding Agents to use the new virtual directory.

10. Select your existing databases to migrate them to VCM 5.4.1.

    If Installation Manager requests that you create a new database, select the previous wizard page and verify that your existing database, which you attached, is selected.

11. Do not select SSL unless your machine is already configured for SSL.

12. After the upgrade is finished, copy the content of `WebConsole\L1033\Files` from your 32-bit Collector to your 64-bit Collector.

    Any existing remote commands, discovery files, and imported template files in this directory are available on the 64-bit Collector.

13. On your 64-bit Collector, run your script to import your VCM scheduled jobs.

14. On your 64-bit Collector, run your script to import your VCM membership logins.

15. Re-import any custom SQL Server Reporting Service Report Definition Language (RDL) files.

What to do next

- Configure the SQL Server settings to tune your VCM database in SQL Server Management Studio, including the VCM database file growth and database recovery. See "Maintaining VCM After Installation" on page 65.
- Log in to VCM.

How to Recover Your Collector Machine if the Migration is not Successful

If the migration to VCM 5.4.1 failed, you must perform several steps to recover your VCM Collector machine. Before you attempt another migration to VCM 5.4.1, contact VMware Technical Support to identify what caused the migration to fail and answer any questions about the migration procedures.

Prerequisites

- Identify the available migration options. See "Migrating VCM" on page 46.
- Understand the scenarios to migrate your VCM environment to VCM 5.4.1. See "Upgrading or Migrating VCM" on page 43.
- Understand the prerequisites to migrate your VCM environment to VCM 5.4.1. See "Prerequisites to Migrate VCM" on page 44.
- Understand how to attach a SQL server database in SQL Server Management Studio. See the Microsoft MSDN Library.

Procedure

1. On your VCM Collector, reinstall the software that was installed before you started the migration. Install the software in the order listed.
   a. SQL Server 2005
   b. SQL Server Reporting Services, 32-bit version
   c. SQL Server 2005 SP3
   d. VMware VCM 5.3, EMC Ionix SCM 5.0 or later, or Configuresoft ECM 4.11.1 or later
2. Use SQL Server Management Studio Object Explorer to connect the databases from your backed up copies.
3. Recopy the files to the `CMFILES$` share.

Upgrading VCM and Components

To prepare your environment for VCM 5.4.1, you can upgrade VCM, Windows Agents, UNIX or Linux Agents, and VCM Remote Clients.

An upgrade to VCM 5.4.1 uses an existing VCM Collector installation. Before you migrate any part of your existing VCM environment to VCM 5.4.1, you must perform several prerequisites.

Prerequisites

- Review and understand the upgrade scenarios. See "Upgrading or Migrating VCM" on page 43.
- Verify that your VCM Collector meets all of the hardware and software requirements for a 64-bit environment. For a list of requirements, see the *VCM Hardware and Software Requirements Guide*.
- Obtain the installation package from the Download VMware vCenter Configuration Manager Web site or the VCM 5.4.1 CD.

Procedure

- "Upgrade VCM" on page 55

  An upgrade to VCM 5.4.1 uses an existing VCM Collector installation. You can upgrade a 64-bit environment that is running VCM 5.3 or earlier to VCM 5.4.1.

- "Upgrade Existing Windows Agents" on page 55

  Use the Upgrade Agent wizard to upgrade the Agent files on one or more Windows machines. If you are upgrading VCM from 5.4, an upgrade to your Windows Agents is not required.

- "Upgrade Existing VCM Remote Clients" on page 56

  The VCM Collector can determine whether the VCM Remote client machine is running an older version of the client software, and can automatically upgrade the version on the client.

- "Upgrade Existing UNIX Agents" on page 57

  Use the UNIX Agent upgrade packages to update the VCM Agents on your UNIX machines. You can use a local package or a remote package to upgrade the UNIX Agents.

- "Upgrade VCM for Virtualization" on page 60

  To upgrade vCenter collections, install the VCM 5.4 Agent or later on the Windows machines running vCenter.

Upgrade VCM

An upgrade to VCM 5.4.1 uses an existing VCM Collector installation. You can upgrade a 64-bit environment that is running VCM 5.3 or earlier to VCM 5.4.1.

Prerequisites

Perform the prerequisites to upgrade VCM on the Collector. See "Upgrading VCM and Components" on page 54.

Procedure

1. On your Collector machine, upgrade the operating system to Windows Server 2008 R2.
2. Uninstall the 32-bit version of SQL Server Reporting Services (SSRS) 2005.
3. Upgrade SQL Server 2005 to SQL Server 2008 R2.
4. Run the SQL Server 2008 R2 installation again and add SSRS 2008.
5. Click **Start**.
6. Select **All Programs > Microsoft SQL Server 2008 R2 > Configuration Tools > Reporting Services Configuration Manager**.
7. Configure SSRS 2008 to use the existing ReportServer database.
   a. Select the existing ReportServer database.
   b. Configure the Web Service and Report Manager URLs.
   c. Select the Encryption Keys option to delete encrypted content so that the new installation of SSRS can use the existing SSRS database.
8. Run the VCM Installation Manager to upgrade the existing VCM software version to 5.4.1.

What to do next

Log in to VCM and upgrade your VCM Windows Agents.

Upgrade Existing Windows Agents

Use the Upgrade Agent wizard to upgrade the Agent files on one or more Windows machines. If you are upgrading VCM from 5.4, an upgrade to your Windows Agents is not required.

The upgrade process uses the current settings of the Agent installed on the Windows machine. For example, if the Agent uses DCOM, or HTTP on port 26542, the upgrade process retains that setting. This process will not upgrade components that do not require an upgrade.

Prerequisites

- Review the supported platforms in the *VCM Hardware and Software Requirements Guide*.
- Install the VCM Agent on the managed machines to upgrade.

Procedure

1. Click **Administration**.
2. Select **Machines Manager > Licensed Machines > Licensed Windows Machines**.
3. Select the Windows machines to upgrade.
4. On the toolbar, click the **Upgrade Agent** icon.
5. On the Machines page, select the Windows machines to upgrade and click the arrow to move the

machines to the Selected pane.

Option	Description
All machines	Upgrades the Agent on all machines that appear in the list of licensed machines.
Filtered machines only	Upgrades the Agent on all machines that appear in the filtered list of machines. This option is only available if the Licensed Machines list is being filtered.
Selected machine(s) only	Upgrades the Agent only on selected individual machines.

6. Click **Next**.
7. On the Install Options page, select or verify the option for the Agent installation and click **Next**.

   The default source of the Agent files is the Collector machine. If you created an Alternate Source, select it from the drop-down list.
8. On the Schedule page, schedule the operation and click **Next**.
9. On the Important page, verify the summary and click **Finish**.

What to do next

Upgrade your VCM Remote clients.

Upgrade Existing VCM Remote Clients

The VCM Collector can determine whether the VCM Remote client machine is running an older version of the client software, and can automatically upgrade the version on the client.

Prerequisites

Install the VCM Agent on the managed machines to upgrade.

Procedure

1. Click **Administration**.
2. Select **Settings > General Settings > VCM Remote**.
3. Select the **Will Remote automatically upgrade old Remote clients?** setting.
4. Click **Edit Setting** and select **Yes**.

   When this setting is enabled, the next contact between the client and server automatically downloads and installs the upgrade files and upgrades the VCM Remote client software on the client machine.

   If the VCM Remote client does not have a certificate, the upgrade process automatically extracts the certificate and sends it to the client, along with the new Agent.
5. Click **Next** and **Finish**.

What to do next

Upgrade your VCM UNIX Agents.

Upgrade Existing UNIX Agents

Use the UNIX Agent upgrade packages to update the VCM Agents on your UNIX machines. You can use a local package or a remote package to upgrade the UNIX Agents.

VCM supports upgrading the UNIX Agent on most UNIX and Linux platforms. Other UNIX platforms are only supported up to a specific Agent version. For a complete list of UNIX Agents supported on UNIX and Linux platforms, see the *VCM Hardware and Software Requirements Guide*.

Prerequisites

- Identify UNIX machines that are not supported for upgrade to the VCM 5.4.1 Agent. See the *VCM Hardware and Software Requirements Guide*.
- Understand Red Hat server and workstation licensing for different versions of VCM. See "Red Hat Server and Workstation Licensing" on page 57.
- Understand VCM support for the Transport Layer Security protocol. See the *VCM Transport Layer Security Implementation* white paper on the Download VMware vCenter Configuration Manager Web site.
- If you install the VCM Agent on HP-UX 11.11 platforms, install patch `PHSS_30966`. For assistance, contact VMware Technical Support.

Procedure

- "Upgrade UNIX Agents Using a Local Package" on page 57

  Use UNIX remote commands and the local Agent package to upgrade the VCM UNIX Agent on the UNIX platforms in your environment.

- "Upgrade UNIX Agents Using a Remote Package" on page 59

  Use VCM remote commands and a remote Agent package to upgrade the VCM UNIX Agent on the UNIX platforms in your environment.

Red Hat Server and Workstation Licensing

When you upgrade the UNIX Agent on Red Hat machines, be aware of the licensing changes between versions of VCM. Prior to VCM 5.2, Red Hat workstations and servers were licensed as Red Hat servers. In VCM 5.2, Red Hat machines were licensed as either workstations or servers.

When you upgrade to VCM 5.2 or later, Red Hat workstations that were previously managed with server licenses are not managed in VCM. Unmanaged Red Hat machines appear in the Available UNIX Machines list before you license them. To license these machines, click **Administration**, select **Machines Manager > Available Machines > Available UNIX Machines**, and re-license the machines using the Linux/Mac Workstation licenses.

For help to identify your unmanaged Red Hat machines, contact VMware Technical Support.

Upgrade UNIX Agents Using a Local Package

Use UNIX remote commands and the local Agent package to upgrade the VCM UNIX Agent on the UNIX platforms in your environment.

The `Agent Upgrade - Local Package` UNIX remote command upgrades existing UNIX Agents when the Agent package exists locally or in a remote location that is accessible by the target machine, such as on a file share.

Prerequisites

- Install the VCM UNIX Agent on the managed machines to upgrade.
- Determine which Agent version is installed on a UNIX machine. Click **Administration** and select **Machines Manager > Licensed Machines > Licensed UNIX Machines**. Select **About > Versions**.

Procedure

1. On your VCM Collector, open Windows Explorer.
2. Select `\Program Files (x86)\VMware\VCM\WebConsole\L1033\Files\UNIX_Remote_Command_Files`.
3. Locate the `AgentUpgradeLocal.sh` UNIX Agent upgrade package.
4. Open `AgentUpgradeLocal.sh` in a text editor.
5. Locate the following entry:

   ```
   CSI_INSTALL_PACKAGE_LOCATION = CHANGE_THIS_TO_A_LOCAL_OR_NFS_DIRECTORY
   ```

6. Change this entry to a local directory or network file share where the VCM Agent installation packages reside.

   For example, `/tmp/VCMu_Agent`.

   Agent installation packages reside on the Collector in `\Program Files (x86)\VMware\VCM\Installer\Packages`.
7. Save and close `AgentUpgradeLocal.sh`.
8. Log in to VCM.
9. Click **Console**.
10. Select **UNIX Remote Commands > UNIX Agent Upgrade**.
11. In the UNIX Agent Upgrade data grid, select **Agent Upgrade - Local Package** and click **Run**.
12. Select the machines on which to upgrade the UNIX Agent.

    To determine which Agent is installed on a UNIX machine, click **Administration** and select **Machines Manager > Licensed Machines > Licensed UNIX Machines**.

    To determine the latest Agent version, select **About > Versions**.
13. Click the arrow button to move the machines from the **Available list** to the **Selected list** and click **Next**.
14. Select whether to upgrade the Agent now or later.

    To change the date, click the **Calendar** icon. When you schedule the action, it appears in the **Administration > Job Manager > Scheduled** list.

    The Time of Day settings are based on your user time zone. All VCM jobs run based on the VCM database time zone. Account for the time and date differences between your VCM user time and your VCM database time. For example, if your VCM database server is in the Eastern time zone, and your VCM user is in the Pacific time zone, to run your job at midnight, enter 9 PM.
15. Click **Next** and **Finish**.

What to do next

Upgrade your UNIX Agents using a remote package. See "Upgrade UNIX Agents Using a Remote Package" on page 59.

Upgrade UNIX Agents Using a Remote Package

Use VCM remote commands and a remote Agent package to upgrade the VCM UNIX Agent on the UNIX platforms in your environment.

The UNIX Agents use Transport Layer Security (TLS) and the Enterprise Certificate is embedded in the Agent package. If multiple Collectors must communicate with a single Agent, all of the Collectors must share an Enterprise Certificate. If the Collectors have different Enterprise Certificates, the Enterprise Certificate from each Collector must be uploaded to the Agent. For more information, see the *VCM Transport Layer Security Implementation* white paper on the Download VMware vCenter Configuration Manager Web site.

The UNIX remote commands use existing configuration settings to upgrade the UNIX Agents using a remote Agent package. VCM sends the Agent package to the target machine.

The remote package sends the UNIX Agent upgrade package with the remote command to execute on the UNIX machine. The following remote upgrade packages are designed specifically for the various operating systems where the Agents can be upgraded.

- AIX 5 Agent Upgrade
- HP-UX (Itanium) Agent Upgrade
- HP-UX (PA-RISC) Agent Upgrade
- Mac OS X Agent Upgrade
- Red Hat Enterprise 3.0, 4.0, 5.0, 5.1, 5.2, and SUSE Enterprise 9 and above Agent Upgrade
- Solaris (SPARC) Agent Upgrade
- Solaris (x86) Agent Upgrade

Older machines use the following packages.

- For AIX 4.3.3 Agent Upgrade, use only `CMAgent.5.1.0.AIX.4`.
- For Red Hat Enterprise 2.1 Agent Upgrade, use only `CMAgent.5.1.0.Linux.2.1`.

The following procedure upgrades the UNIX Agents using one of the remote upgrade packages.

Prerequisites

Install the VCM UNIX Agent on the managed machines to upgrade.

Procedure

1. Click **Console**.
2. Select **UNIX Remote Commands > UNIX Agent Upgrade**.
3. In the UNIX Agent Upgrade data grid, click the appropriate remote upgrade package for the operating system and version of the machines to upgrade.
4. Click **Run** and follow the wizard to send the remote command and upgrade package to the Agents on the selected machines.

   The Agent executes the upgrade package.

What to do next

Upgrade VCM for Virtualization. See "Upgrade VCM for Virtualization" on page 60.

Upgrade VCM for Virtualization

To upgrade vCenter collections, install the VCM 5.4 Agent or later on the Windows machines running vCenter.

When you upgrade a Collector to VCM 5.4.1, the Agent Proxy on the Collector is automatically upgraded and the Agent Proxy protected storage and user account configuration settings are preserved. For existing non-Collector Agent Proxy machines, you must upgrade VCM for Virtualization and retain the Secure Communication settings.

Prerequisites

- Do not change the password for the CSI Communication Proxy service when you upgrade VCM for Virtualization. If you change the password, you might need to reinstall and reconfigure the Agent Proxy.
- Do not install the Agent Proxy and Active Directory on the same machine. The operations required to install, uninstall, upgrade, and reinstall these products can cause you to reinstall and reconfigure the Agent Proxy.
- Before you uninstall VCM for Virtualization manually, you must execute `RetainSecureCommSettings.exe`. Otherwise, the Agent Proxy configuration settings will be removed, and you will need to reconfigure the Agent Proxy. The `RetainSecureCommSettings.exe` is located in `C:\Program Files (x86)\VMware\VCM\Installer\Packages`, or in the path relative to where you installed the software. For more information, see "Configure vCenter Server Data Collections" on page 143.

Procedure

To upgrade the VCM for Virtualization Agent Proxy on non-Collector machines, use one of these methods depending on your configuration.

- "Use VCM to Upgrade an Agent Proxy Machine" on page 60

  Use VCM to upgrade VCM for Virtualization on a non-Collector Agent Proxy Machine. If a new version of the Agent Proxy becomes available, the upgrade process installs the newer version on your Agent Proxy machine.

- "Manually Upgrade an Agent Proxy Machine" on page 61

  Manually upgrade VCM for Virtualization on a non-Collector Agent Proxy Machine. Use this method to upgrade an Agent Proxy machine if you do not use the upgrade option in VCM.

Use VCM to Upgrade an Agent Proxy Machine

Use VCM to upgrade VCM for Virtualization on a non-Collector Agent Proxy Machine. If a new version of the Agent Proxy becomes available, the upgrade process installs the newer version on your Agent Proxy machine.

Procedure

1. On your VCM Collector, click **Administration**.
2. Select **Machines Manager > Additional Components > Agent Proxies**.
3. In the Agent Proxies data grid, select the machines on which to upgrade the Agent Proxy.
4. Click **Upgrade**.
5. On the Upgrade Agent Proxies Machines page, select an action and click **Next**.

Option	Description
All Machines	Runs the process on all eligible machines.
Selected Machines Only	Runs the process on all machines listed in the lower pane.
Filtered Machines	Creates a filter based on the machine name or domain name.
Arrow buttons	Moves a selected machine name between panes.

6. On the Option page, configure the options and click **Next**.

Option	Description
Install From	Selects the name of the Collector used to manage virtual machines.
Schedule	Sets the schedule to run the action.

7. On the Important page, review the summary, click **Back** to make any necessary alterations, and click **Finish**.

   VCM upgrades the Agent Proxy at the specified time.

What to do next

Verify that the upgrade process finished. Click **Jobs** to display the Jobs Summary. To verify jobs for the past 24 hours click **Administration** and select **Job Manager > History > Other Jobs > Past 24 Hours**.

Manually Upgrade an Agent Proxy Machine

Manually upgrade VCM for Virtualization on a non-Collector Agent Proxy Machine. Use this method to upgrade an Agent Proxy machine if you do not use the upgrade option in VCM.

After the upgrade, all managed Windows machines include the VCM Agent extension for VCM Provisioning.

Prerequisites

- Upgrade your Collector to VCM 5.4.1.
- Confirm that `\VMware\VCM\AgentFiles\CMAgentInstall.exe` is accessible from your non-Collector Agent Proxy machine. The path on the Collector machine is `C:\Program Files (x86)\VMware\VCM\AgentFiles\CMAgentInstall.exe`, or in the path relative to where you installed the software.
- For Agent Proxy machines, if the Virtualization proxy and VCM Agent extensions for Provisioning are installed, you must run `ProvisioningProductInstall.exe` from the VCM Collector.
- If you previously used this Agent Proxy to collect data from your upgraded Collector, the first collection might fail because of password encryption. If the collection fails, reset the VM Host password. You can set the password for multiple hosts at the same time. Click **Administration** and select **Machines Manager > Additional Components > VCM for Virtualization > Licensed VM Hosts**.

Procedure

1. On your Agent Proxy machine, execute `CMAgentInstall.exe`.
2. When the installer detects the previous version of VCM and requests permission to uninstall it, select **Yes**.
3. When the installer detects that Secure Communication is installed and requests whether you want to retain your settings, select **Yes**.

   The installer removes VCM for Virtualization and the VCM Agent from your Agent Proxy machine. During this process, your Secure Communication settings are retained.
4. When the installer displays the license agreement, read and accept the conditions.
5. When the installer prompts whether to perform the installation of the VCM Windows Agent in HTTP mode, select **Allow HTTP** and click **Next**.

   Allowing HTTP communication enables the Agent to communicate through the HTTP port if DCOM is not available. Locking an Agent prevents the Agent from being removed or upgraded.
6. When the VCM Windows Agent is installed, click **Finish**.
7. Copy the Virtualization product installation executable file from your upgraded Collector machine to any location on your non-Collector Agent Proxy machine.

   The path to this file is as follows, or is in the path relative to where you installed the software.

   ```
   C:\Program Files
   (x86)\VMware\VCM\AgentFiles\Products\VirtualizationProductInstall.exe
   ```
8. On your non-Collector Agent Proxy machine, run `VirtualizationProductInstall.exe` to install VCM for Virtualization.
9. When VCM for Virtualization is installed, click **Finish**.

What to do next

Use your upgraded Agent Proxy to collect data from managed machines.

Unregister the Previous Version of the vSphere Client VCM Plug-In

Before you upgrade to the new version of the vSphere Client VCM Plug-In that is available when you upgrade VCM, you must unregister a previous version of the plug-in.

The VCM upgrade removes the previous plug-in files and installs the new plug-in files in new locations with new names. The VCM upgrade does not register the new plug-in with the vSphere Client.

Procedure

1. On your Collector machine, navigate to `C:\Program Files (x86)\VMware\VCM\Tools\vSphere Client VCM Plug-in\bin`.
2. Double-click `VCVPInstaller.exe`.
3. In the VMware vSphere VCM Plug-in Registration dialog box, click **Unregister**.
4. In the Server URL field, enter the name of your vCenter Server.

   For example, `https//vcenter05/sdk`.
5. In the Administrator User Name and Password fields, enter the Administrator user name and password.
6. Click **OK**.

What to do next

Upgrade the vSphere Client VCM Plug-In. See "Upgrade the vSphere Client VCM Plug-In" on page 63.

Upgrade the vSphere Client VCM Plug-In

If your version of the plug-in is 5.3 or earlier, or if the URL to the VCM instance has changed, upgrade the vSphere Client VCM Plug-In.

Prerequisites

- Unregister the previous version of the vSphere Client VCM Plug-In. See "Unregister the Previous Version of the vSphere Client VCM Plug-In" on page 62.
- Locate the procedure to upgrade VCM. See "Upgrading VCM and Components" on page 54.

Procedure

1. Upgrade VCM.

What to do next

Register the new vSphere Client VCM Plug-In. See "Register the vSphere Client VCM Plug-In" on page 163.

Maintaining VCM After Installation 5

Perform routine maintenance on your VCM configuration management database (CMDB) to keep VCM running smoothly and performing efficiently. Maintenance includes configuring settings specific to your environment, configuring the database file growth and recovery settings, creating a maintenance plan, and incorporating the database into your backup and disaster recovery plans.

Prerequisites

- Install VCM. See "Installing VCM" on page 19.
- Understand the database recovery models. See "Database Recovery Models" on page 67.

Procedure

1. "Customize VCM and Component-Specific Settings" on page 65

   Customize the general VCM settings and the component-specific settings for your environment.

2. "Configure Database File Growth" on page 67

   Configure the autogrowth properties of the VCM database and log file to restrict the file growth from affecting VCM performance.

3. "Configure Database Recovery Settings" on page 68

   SQL Server supports several database recovery models to control transaction log maintenance. Set a specific recovery model for each database.

4. "Create a Maintenance Plan for SQL Server 2008 R2" on page 69

   To ensure that VCM runs at peak performance and requires little operator intervention during its lifecycle, you must set up a routine maintenance plan. VCM relies heavily on its SQL databases for operation.

5. "Incorporate the VCM CMDB into your Backup and Disaster Recovery Plans" on page 70

   Consider your VCM configuration management database as any other SQL database in your environment and incorporate the database into your corporate strategy for backup and disaster recovery.

Customize VCM and Component-Specific Settings

Customize the general VCM settings and the component-specific settings for your environment.

You can customize general settings for the VCM Collector, customer information, database, input or output directories, VCM Remote, the VCM installer, auditing, and operating system patching. You can customize specific settings for installed and licensed components.

Procedure

1. On your VCM Collector, select **Administration**.
2. Click **Settings** and review the available general and product-specific configuration settings to customize for your environment.
3. Click **Windows** and configure the settings to communicate with the VCM Windows Agent for your collection types.

Option	Description
Agent - General	Configures the general characteristics of the Windows Agent operation.
Agent - Thread Priority	Configures priorities for collections while running on managed machines.
Data Retention	Configures the time to retain each VCM data type in the database.
Custom Information	Displays the Windows Custom Information script and output types.

4. Click **UNIX** and configure the settings to communicate with the VCM UNIX Agent for your collection types.

Option	Description
Agent - General	Configures the general characteristics of the UNIX Agent operation.
Agent - RunAsSuid	Configures data types as RunAsSuid for selected operating systems during Agent operation.
Agent - Nice	Configures the Nice settings for each data type during Agent operation.
Data Retention	Configures the time to retain each VCM data type in the database.
Custom Information Types	Adds custom data types and directives to collect data and parse text files.
Restricted Path	Configures restricted paths for editing file properties.

5. For the products that you licensed and the network authority, review and update the component-specific settings for your environment.

Option	Description
Asset Extensions	Configures the hardware device and software configuration item settings.
Integrated Products	Configures settings for the VMware and EMC products that integrate with VCM.
OS Provisioning	Enables OS provisioning and configures the server connection timeout and user account.
VCM for Active Directory	Configures the data retention settings for AD objects and the AD display settings.
VCM for Exchange	Configures the Agent general and thread priority settings to communicate with the VCM Windows Agent, and the Exchange data retention and trending settings.
VCM for Virtualization	Configures the data retention settings for vCenter, virtual machine hosts and guests, and the virtual machine logs.

Option	Description
Network Authority	Configures and manages the available domains, available accounts, and assigned accounts by domain or machine group, and the proxy servers used during the HTTP Agent installation.

What to do next

- See the online help for each product component for more information about the specific settings.
- Configure the database file growth. See "Configure Database File Growth" on page 67.

Database Recovery Models

SQL Server supports several database recovery models to control transaction log maintenance. You set a specific model to each database. The VCM database settings are set to **Simple** by default. Retain these settings for all VMware databases, and use the nightly full or incremental backups.

- **Simple Recovery:** The VCM database settings are set to **Simple** by default. The transaction log retains enough information to recover the database to a known good state when the server restarts. Transaction log backups are not allowed and point-in-time recovery is not available. Simple recovery causes the transaction log file to grow. SQL Server is in Auto Truncate mode, so the log file periodically rolls over as data moves from the log file to the data file.
- **Bulk Logged Recovery:** The transaction log retains all normal transaction information and discards transactions that result from a bulk operation. VCM uses the `IROWSETFASTLOAD` interface extensively, which is bulk logged.
- **Full Recovery:** The transaction log retains all information until it is purged through the SQL Server LOG backup operation, which the database administrator uses to perform point-in-time recovery. Full recovery allows incremental backups of the database. Do not use point-in-time recovery because certain factors in VCM weaken the point-in-time recovery model. If you implement Full Recovery, you must set up scheduled daily backups of the transaction log. The log files will continue to grow and accumulate changes until you back them up. A Full Recovery database that does not have scheduled backups can fill its disk and stop the system.

Configure Database File Growth

Configure the autogrowth properties of the VCM database and log file to restrict the file growth from affecting VCM performance.

The VCM installer creates a 2GB data file and a 1GB log file. These files grow as ongoing operations add data to VCM.

The file growth for each file is set to the default value for Microsoft SQL Server 2008 R2. In some environments, these default values can result in file fragmentation or reduced performance. The following procedure sets the autogrowth property in each database.

Prerequisites

Understand the database recovery models. See "Database Recovery Models" on page 67.

Procedure

1. Click **Start**.
2. Select **All Programs > Microsoft SQL Server 2008 R2 > SQL Server Management Studio**.
3. Expand the SQL instance.
4. Expand **Databases**.
5. Right-click **VCM** and select **Properties**.
6. In the left pane, select **Files**.
7. In the Autogrowth column, click the ellipsis button.
8. Select **Enable Autogrowth**.
9. In the File Growth area, select **In Percent** and type or select **10**.

   A value of 10% allows the transaction log file to grow by 10% of its current size. This value is critical in large environments where the log file can increase significantly even when using the Simple recovery model.

   Reserve as much space as possible for your transaction log file so that it does not ever have to grow. This configuration will result in the best performance.
10. In the Maximum File Size area, select **Unrestricted File Growth** and click **OK**.
11. Repeat this procedure for **VCM_Log**.

What to do next

Return to the database list and set the **AutoGrowth** value for all VCM-related databases.

Configure Database Recovery Settings

SQL Server supports several database recovery models to control transaction log maintenance. Set a specific recovery model for each database.

The VCM database settings are set to **Simple** by default. If you change the VCM database recovery setting to **Full**, you must manage your own log backups.

Prerequisites

Understand the database recovery models. See "Database Recovery Models" on page 67.

Procedure

1. Click **Start**.
2. Select **All Programs > Microsoft SQL Server 2008 R2 > SQL Server Management Studio**.
3. Expand the **SQL instance**.
4. Expand **Databases**.
5. Right-click **VCM** and select **Properties**.
6. Click **Options**.
7. In the Recovery model drop-down, select the recovery model and click **OK**.

What to do next

Create a maintenance plan for SQL Server 2008 R2. See "Create a Maintenance Plan for SQL Server 2008 R2" on page 69.

Create a Maintenance Plan for SQL Server 2008 R2

To ensure that VCM runs at peak performance and requires little operator intervention during its lifecycle, you must set up a routine maintenance plan. VCM relies heavily on its SQL databases for operation.

The maintenance plan uses the automated maintenance functions on SQL Server 2008 R2 servers that host the VCM database.

Procedure

1. Click **Start**.
2. Select **All Programs > Microsoft SQL Server 2008 R2 > SQL Server Management Studio**.
3. Expand the Management folder, right-click **Maintenance Plans** and select **Maintenance Plan Wizard**.
4. On the Maintenance Plan wizard page, click **Next**.
5. On the Select Plan Properties page, enter a maintenance plan name, select **Single schedule for the entire plan or no schedule**, and click **Change**.
6. On the Job Schedule Properties - Maintenance Plan page, set the scheduling properties to run the maintenance plan when the SQL server is idle or has low usage.
7. Click **OK** to return to the Select Plan Properties page and click **Next**.
8. On the Select Maintenance Tasks page, select the following maintenance tasks and click **Next**.
   - Check Database Integrity
   - Rebuild Index
   - Update Statistics
   - Clean Up History
9. On the Select Maintenance Task Order page, order the maintenance tasks and click **Next**.
10. On the Define Database Check Integrity Task page, define how the maintenance plan will check the database integrity.
    a. Click the Databases drop-down menu.
    b. Select the following databases and click **OK**.
       - CSI_Domain
       - VCM
       - VCM_Coll
       - VCM_Raw
       - VCM_UNIX

       You must select the VCM_Raw database because it contains transient data that the other databases consume.
    c. Select **Include indexes** and click **Next**.
11. On the Define Rebuild Index Task page, define how the maintenance plan will rebuild the Index.

a. Click the Databases drop-down menu.

b. Select the following databases and click **OK**.

- CSI_Domain
- VCM
- VCM_Coll
- VCM_UNIX

Do not rebuild the index for the VCM_Raw database.

c. In the Advanced options area, select **Sort results in tempdb** and click **Next**.

12. On the Define Update Statistics Task page, define how the maintenance plan will update the database statistics.

a. Click the Databases drop-down menu.

b. Select the following databases and click **OK**.

- CSI_Domain
- VCM
- VCM_Coll
- VCM_UNIX

Do not update statistics for the VCM_Raw database.

13. On the Define History Cleanup Task page, define how the maintenance plan will clean up historical data from the SQL Server 2008 R2 machine and click **Next**.

a. Select **Backup and restore history**.

b. Select **SQL Server Agent job history**.

c. Select **Maintenance plan history**.

d. Set the cleanup task to remove historical data older than **4 Months**.

14. On the Select Report Options page, save a report of the maintenance plan actions.

a. Select **Write a report to a text file**.

b. Select a folder for the report and click **Next**.

15. On the Complete the Wizard page, verify your selections in the Maintenance Plan Wizard summary, expand the selections to view the settings, and click **Finish**.

16. When the Maintenance Plan Wizard progress is finished, verify that each action is successful.

What to do next

- You have established a routine maintenance plan to ensure that SQL Server 2008 R2 continues to operate efficiently. To view, save, copy, or send the report, click **Report** and select an option.
- Use VCM normally.

Incorporate the VCM CMDB into your Backup and Disaster Recovery Plans

Consider your VCM configuration management database as any other SQL database in your environment and incorporate the database into your corporate strategy for backup and disaster recovery.

Getting Started with VCM Components and Tools

6

When you use VCM, you must understand user access, how to start VCM from any physical or virtual machine, and familiarize yourself with the VCM portal features.

- "Understanding User Access" on page 71

  User access determines who has access to VCM and with what roles.

- "Log In to VCM" on page 72

  Access VCM from any physical or virtual machine in your network.

- "Getting Familiar with the Portal" on page 73

  The VCM portal provides access to all VCM features to manage your environment.

Understanding User Access

User access determines who has access to VCM and with what roles. To manage your user access, you create rules that are assigned to roles. The roles are then assigned to each user login you create in VCM. User access is managed in the Administration User Manager node.

The user account that was used to install VCM is automatically granted access to VCM, placed in the roles of ADMIN and USER, and placed into the Admin role. This user can log in to VCM using the Admin role. The AD_Admin role allows full administration access to AD objects only.

When a user is added to the Admin role in VCM or granted access to the Administration User Manager node, that user is placed in the fixed machine roles Security Administrators and Bulk Insert Administrators Groups. They are also added to the database roles of public, ADMIN, and User in the VCM Database.

Users who will not have access to the Administration User Manager node will be assigned to public. Depending on the functions granted to a user, they might need additional or fewer privileges for their role to function properly.

VCM provides a Change Restricted role to limit users from making certain changes in your environment. With this role, users can discover, collect data from machines, assess machines, display bulletin and template details, check for updates, and view history. Users can add, edit, and delete reports, compliance rules and rule groups, and compliance and patch assessment templates. They can also install the Agent, upgrade VCM, and uninstall VCM.

When you apply the VCM Change Restricted role to a user's VCM login, they cannot perform the following actions.

- Remote command execution
- Change actions against target managed machines
- Change rollback
- Compliance enforcement
- Patch deployment
- Software deployment
- OS provisioning
- Machine reboots

All VCM user accounts must have the following rights on the VCM Collector machine.

- Ability to log on locally to access IIS
- Read access to the `System32` folder
- Write access to the `CMFiles$\Exported_Reports` folder to export reports
- If default permissions have been changed, read access to the `C:\Program Files (x86)\VMware\VCM\WebConsole` directory and all subdirectories and files

  Users who add machines to VCM using a file or the Available Machines Add Machines action must have write access to `CMFiles$\Discovery_Files`.

Running VCM as Administrator on the Collector

By default for localhost, Internet Explorer on Windows Server 2008 R2 runs with Protected Mode enabled. If you are logged in to VCM as an Administrator, because Protected Mode is enabled, problems can occur with the SQLServer Reporting Service (SSRS) Web service interface components such as dashboards and node summaries, or when you use the License Manager Click Once application.

When you update a VCM license using the License Manager application from the Collector's Web console, you must run Internet Explorer as administrator.

CAUTION Although you should not access VCM on the Collector using a Web console, to restore the SSRS and License Manager functionality you can run Internet Explorer as administrator or disable Protected Mode for the zone of the Collector (localhost). If you perform either of these actions, you must take additional precautions to protect the Collector because of the increased exposure to attacks on the Collector through the Web browser, such as cross-site scripting.

Log In to VCM

Access VCM from any physical or virtual machine in your network. The level of access is determined by your VCM administrator.

Prerequisites

- Verify that the physical or virtual machines from which you are accessing VCM have a supported version of Internet Explorer installed. For supported platforms, see the *VCM Hardware and Software Requirements Guide*.
- Configure the Internet Explorer Pop-up Blocker settings to add your Collector to your list of allowed Web sites, or disable Pop-up Blocker. Click **Internet Explorer** and select **Tools > Pop-up Blocker > Pop-up Blocker Settings** and then add the path for your Collector in the allowable address field.

Procedure

1. To connect to VCM from a physical or virtual machine on your network, open Internet Explorer and type `http://<name_or_IP_of_Collector_machine>/VCM`.
2. Type your user network credentials.
3. (Optional) Select **Automatically log on using this role** to have VCM automatically log you on without prompting you for a role in future logons.
4. Click **Log On**.

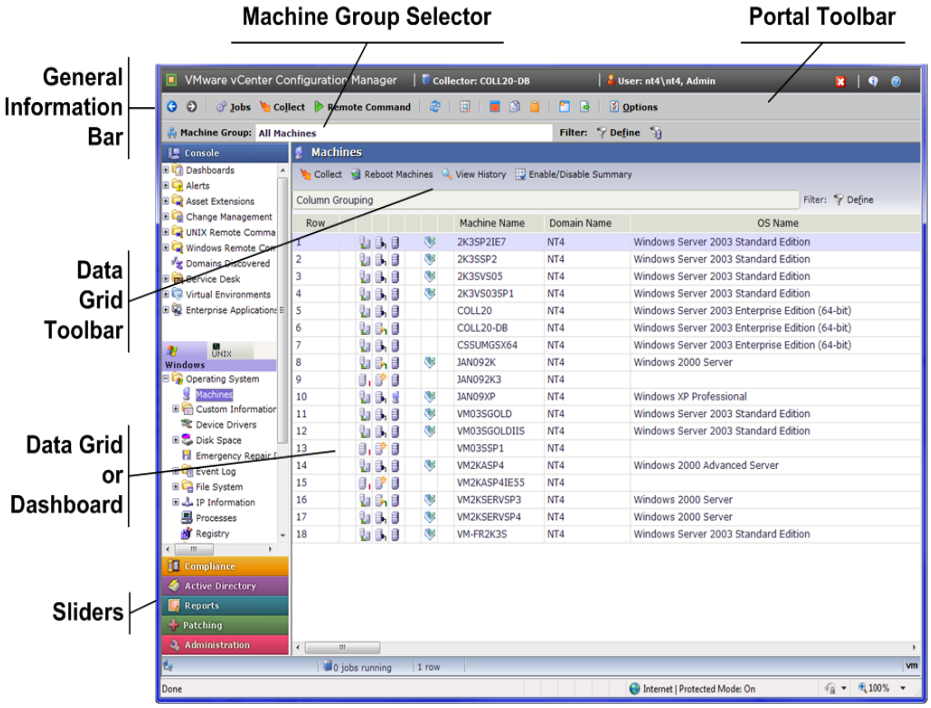
Your VCM user account may have multiple roles. If you selected the **Automatically log on using this role** option, VCM will automatically log you on as the User Role displayed on the Logon screen. To change roles, you must use the Logoff button in the top right corner of the Console. This action will return you to the Logon screen so that you can use the drop-down menu to select a different role.

Getting Familiar with the Portal

The VCM portal provides access to all VCM features to manage your environment.

The portal uses a browser-based interface to run from any Windows machine that has access to the server on which VCM is installed. The Windows machine must be running Internet Explorer or Mozilla Firefox with the Internet Explorer tab plug-in installed.

The Portal includes several major areas and controls.



General Information Bar

The general information bar displays the VCM Collector's active SQL Server name, your VCM user name and active Role, and the following buttons.

- **Log Out:** Exits the Portal. The Portal closes and the VCM Logon screen appears.
- **About:** Displays information about how to contact VMware Technical Support and version information for VCM and all of its components. This information may be important when you contact VMware Technical Support.
- **Help:** Opens the online Help for the currently-active display.

Portal Toolbar

The global toolbar provides you with easily-accessible options to enhance control of your environment and data.

	The left and right arrow buttons navigate to the previous or next page in the data area.
	The Jobs button opens the Jobs Running status window. This button provides access to the Collector status and allows you to stop and restart the Collector service.
	The Collect button opens a wizard that allows you to define and initiate data collections.
	The Remote Commands button allows you to invoke the Remote Commands wizard from the toolbar without having to access the node.
	The Refresh data grid view button refreshes the data grid. Press F5 on the keyboard as an alternative action.
	The View row cells button displays a vertically scrolling view of a single row of data, rather than the table-based data grid view in a separate window, and allows you to move between records.
	The Select all displayed data rows button selects all the rows in the data grid.
	The Copy button copies information from the selected rows in the data grid to the clipboard.
	The Copy link to clipboard button copies the link of the content on-screen to the clipboard.
	The View data grid in separate window button displays the data grid in a separate window.
	The Export displayed data button exports data to a CSV formatted file. This file is exported to `\\<name_of_Collector_machine>\CMfiles$\Exported Reports`.
	The Options button opens the User Options window. These settings pertain to the User who is logged in to VCM. All VCM users can configure these settings to their individual preferences.

Sliders

The sliders on the left side of the Portal include the items listed and described in the following table. The individual items that you see in VCM will vary depending on the components that you have licensed.

- Active Directory and AD objects are available only when VCM for Active Directory (AD) is licensed. This slider is viewable based on your role.
- Patching options are available only when VCM Patching is licensed. This slider is viewable based on your role.
- Administration is visible only to users who have Administrative rights to VCM as part of their VCM role.

For detailed instructions about any of these features, see the online Help.

Slider	Action
Console	■ View, export, or print enterprise-wide, summary information. ■ Review or acknowledge current alert notifications. ■ Manage VCM discovered and non-VCM discovered hardware and software assets. ■ Review changes that occurred from one collection to the next. ■ Create, edit, or run remote commands on a VCM managed Windows or UNIX machine. ■ View information about VCM discovered domains. ■ Navigate and manage integrated service desk events. ■ Manage virtual machines. ■ View your Windows NT Domain and Active Directory related data. ■ View information for enterprise-level applications. ■ Review non-security related UNIX machine-specific information. ■ Review UNIX security data to ensure consistent security configurations across your environment.
Compliance	■ Create and manage Compliance rule groups and templates based on AD objects or machine group data.
Active Directory	■ View, export, or print enterprise-wide, summary information for Active Directory objects. ■ Review alert notifications for the selected AD location. ■ Review Active Directory-related changes that occurred from one collection to the next. ■ View collected information about Active Directory objects such as Users, Groups, Contacts, Computers, Printers, Shares, and Organizational Units. ■ Review Active Directory site lists, including Site Links, Site Link Bridges, Subnets, Intersite Transports, Servers, Connections and Licensing. ■ View Active Directory Group Policy Container Settings. ■ View information about Active Directory Domains, DCs, and Trusts. ■ Track and display access control entries and security descriptor data on all collected

Slider	Action
	objects. ■ View Active Directory Schema information.
Reports	■ Run out-of-the-box reports against your collected data. ■ Write your own SQL and SSRS reports using VCM's report wizard.
Patching	■ Review a list of Microsoft bulletins available to VCM. ■ Create, run, or import VCM Patching templates to display the machines that require the patches described in each bulletin. ■ Select machines to license, set options for assessment and deployment, or monitor VCM Patching jobs. ■ Deploy patches.
Administration	■ Manage basic configuration options for VCM. ■ Establish filters to limit the data you collect from machines in your environment. ■ Manage your VCM licenses. ■ Identify and manage your physical and virtual machines using VCM. ■ Manage VCM Logins and Roles. ■ View the status of jobs that are currently running, scheduled to run, or completed. ■ Configure VCM to notify you of certain conditions in your environment.

Getting Started with VCM 7

Before you can use VCM to manage the machines in your enterprise, you must complete several steps.

1. Discover, License, and Install Windows Machines.
2. Discover, License, and Install UNIX/Linux Machines.
3. Discover, License, and Install Mac OS X Machines.
4. Discover, Configure, and Collect Oracle Data from UNIX Machines.
5. Customize VCM for your Environment.
6. Set up and use VCM auditing.

Discover, License, and Install Windows Machines

Discover, License, and Install Windows Machines

To manage your Windows machines, you must verify domains and accounts, discover and license those machines, install the VCM Agent, and collect Windows data from those machines. You can also collect Windows Custom Information.

Procedure

1. Verify Available Domains

   Allow VCM access to each domain so that the VCM Collector can interact with the Windows machines in your environment.

2. Check the Network Authority

   Verify that at least one domain account with administrator privileges is available to act as a network authority account for VCM.

3. Assign Network Authority Accounts

   Select and assign the network authority account that you identified for VCM access to the Windows machines.

4. Discover Windows Machines

   Identify the Windows machines in your network that you are managing with VCM.

5. License Windows Machines

   To manage Windows machines, you must license them in VCM.

6. Disable User Account Control for VCM Agent Installation

Disable User Account Control (UAC) on Windows 7, 2008, 2008 R2, and Vista target machines before you install the VCM Agent.

7. Install the VCM Windows Agent on Your Windows Machines

   Install the VCM Windows Agent on each Windows machine to manage.

8. Enable UAC After VCM Agent Installation

   Enable User Account Control (UAC) on Windows 7, 2008, 2008 R2, and Vista machines after you install the VCM Agent.

9. Collect Windows Data

   Start managing the Windows machines by performing an initial collection, which adds Windows machine data to VCM.

Continuous Windows machine management is based on the latest data you collect from target machines. You can view data and run actions, such as reports or compliance, based on the collected data. See "Windows Collection Results" on page 91.

Verify Available Domains

Allow VCM access to each domain so that the VCM Collector can interact with the Windows machines in your environment.

During installation, VCM discovered all domains to which the network authority account had access. If the Windows machines belong to a domain that is not listed, you must add that domain manually.

Prerequisites

Know the fully-qualified names of the domains to manage.

Procedure

1. Click **Administration**.
2. Select **Settings > Network Authority > Available Domains**.
3. Verify that the domain appears in the Available Domains view.
4. If the domain does not appear, add the domain.
   a. Click **Add**.
   b. Type the domain name and select the domain type as **NetBios** or **AD**, depending on your domain, and click **OK**.

What to do next

Verify that a network authority account is available and create other necessary domain accounts. See "Check the Network Authority" on page 78.

Check the Network Authority

Verify that at least one domain account with administrator privileges is available to act as a network authority account for VCM.

Although you specified an initial default network authority account when you installed VCM, you can add different administrator accounts if you do not assign the default account.

Prerequisites

Verify the presence of domains. See "Verify Available Domains" on page 78.

Procedure

1. Click **Administration**.
2. Select **Settings > Network Authority > Available Accounts**.
3. To add a new domain account, click **Add**.
4. Type the domain name, user name, and password, and click **Next**.
5. Click **Finish** to add the account.

What to do next

Assign the network authority account to the domain so that VCM can access the Windows machines in the domain. See "Assign Network Authority Accounts" on page 79.

Assign Network Authority Accounts

Select and assign the network authority account that you identified for VCM access to the Windows machines.

You can assign a single account to all domains and machine groups, or assign a unique account or multiple accounts to each domain and machine group.

Use the following NetBios procedure as a guideline.

Prerequisites

Verify or add the necessary network authority account. See "Check the Network Authority" on page 78.

Procedure

1. Click **Administration**.
2. Select **Settings > Network Authority > Assigned Accounts > By Domain > NetBios**.
3. Select an assigned account.
4. Click **Edit Assigned Accounts**.
5. Select the account to receive authority to the domain and click **Next**.
6. Confirm the accounts to include in the authority list for the domain and click **Finish**.

What to do next

Discover the Windows machines in your environment. See "Discover Windows Machines" on page 79.

Discover Windows Machines

Identify the Windows machines in your network that you are managing with VCM.

To discover the available Windows machines, VCM uses general discovery rules to identify many Windows machines or specific discovery rules to identify particular Windows machines.

The time required to perform an initial discovery depends on the size and composition of your network. If all Windows machines are not available during initial discovery, such as systems that are disconnected from the network, the first discovery will not find all Windows machines. If the discovery does not identify all Windows machines, you might need to run additional discoveries after the other Windows machines become available.

NOTE The Discovered Machines Import Tool (DMIT) can import many physical and virtual machines at one time into the VCM database. The tool imports machines discovered by the Network Mapper (Nmap). Download DMIT from the VMware Web site.

The following procedure is based on Active Directory.

Prerequisites

Assign a Network Authority Account that VCM can use for access. See "Assign Network Authority Accounts" on page 79.

Procedure

1. Click **Administration**.
2. Select **Machines Manager > Discovery Rules**.
3. Click **Add** to create a discovery rule.
4. On the Discovery Rules page, type a name and description and click **Next**.
5. On the Discovery Method page, select **By Active Directory** and click **Next**.
6. On the AD Domain page, specify the AD Domain, select **Discover machines only from the selected domain**, and click **Next**.
7. On the Discovery Filters page, select **Discover all machines in <domain_name> Domain**.
8. (Optional) Create a filter to discover Windows machines based on a limited criteria and click **Next**.
9. On the Important page, click **Yes** and **Finish**.

   To avoid exceeding your license count, do not select **License and Install Agent on Discovered Machines**.
10. On the toolbar, click **Jobs** to track current discovery job status.

    The Jobs Running window displays the job name and summary information while the job runs.

What to do next

- Verify that jobs have finished running. Click **Administration** and select **Job Manager > History > Other Jobs > Past 24 Hours**.
- Verify that the Windows machines are available. Click **Administration** and select **Machines Manager > Available Machines > Available Windows Machines**.
- License the Windows machines in your environment. See "License Windows Machines" on page 80.

License Windows Machines

To manage Windows machines, you must license them in VCM.

The number of discovered Windows machines might exceed the number of your available licenses. If that happens, a message appears indicating that not enough licenses are available.

Prerequisites

Verify that the Windows machines you are licensing are listed with a machine type of workstation or server in **Available Windows Machines** in the following procedure. If the type is not workstation or server, VCM cannot license the machines. Contact VMware Technical Support to resolve a machine type that is not recognized by VCM.

Procedure

1. Click **Administration**.
2. Select **Machines Manager > Available Machines > Available Windows Machines**.
3. Select the Windows machines to license.
4. Click **License**.
5. Verify that the Windows machines to license appear in the Selected list.

   Use the arrows to move the Windows machines.
6. When you initially license Windows machines, do not select the **Install VCM Agents for the selected machines** check box.
7. Click **Next** to view your Product License Details.

   The licensed Windows machine count increases by the number of licensed machines.
8. Click **Next**.

   VCM confirms that the licenses you requested will be applied to the selected Windows machines.
9. Click **Finish**.

What to do next

Disable User Account Control (UAC) on the Windows 7, 2008, 2008 R2, or Vista machines in your environment. See "Disable User Account Control for VCM Agent Installation" on page 81.

Disable User Account Control for VCM Agent Installation

Disable User Account Control (UAC) on Windows 7, 2008, 2008 R2, and Vista target machines before you install the VCM Agent.

The UAC setting on Windows 7, 2008, 2008 R2, and Vista machines prevents VCM from installing the Agent on these target machines. You can disable UAC on a single Windows machine or a group of machines.

- "Disable User Account Control for a Windows Machine" on page 81
- "Disable User Account Control By Using Group Policy" on page 82

Disable User Account Control for a Windows Machine

The User Account Control (UAC) on Windows 7, 2008, 2008 R2, or Vista machines prevents VCM from installing the Agent on the target machines. Before you install the Agent on a Windows 7, 2008, 2008 R2, or Vista machine, you must disable the UAC, and then re-enable UAC after you finish the installation.

This procedure disables UAC on a Windows 2008 R2 machine.

Procedure

1. On the target Windows 2008 R2 machine, click **Start > Run**.
2. In the Run dialog box, type **msconfig** and click **OK**.
3. In the User Account Control dialog box, click **Continue**.

4. In the System Configuration dialog box, click the **Tools** tab.
5. In the Tool Name list, select **Disable UAC**.
6. Click **Launch**.
7. When the command is finished running, click **Close** and click **Close** again.
8. Restart the Windows machine to apply the changes.

What to do next

Install the VCM Windows Agent on licensed Windows machines in your environment, and then enable UAC on the target machine. See "Install the VCM Windows Agent on Your Windows Machines" on page 83.

Disable User Account Control By Using Group Policy

The User Account Control (UAC) on Windows 7, 2008, 2008 R2, and Vista machines prevents VCM from installing the Agent on the target machines.You can use a group policy to disable UAC on the Windows machines in your environment.

The following procedure is performed on a Windows 2008 R2 domain controller machine.

Prerequisites

Configure Windows 7, 2008, 2008 R2, and Vista machines that are targeted for the Agent installation into a common Active Directory domain or organizational unit (OU).

Procedure

1. On your Windows 2008 R2 domain controller, click **Start** and select **Administrative Tools > Group Policy Management**.
2. Click **Forest** and select **Domains > your local domain > Default Domain Policy**.
3. In the Default Domain Policy pane, click the **Settings** tab.
4. Right-click **Policies** and click **Edit**.
5. In the Console Root, expand the domain/OU.
6. Browse to **Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Security Options**.
7. In the right pane, locate the **User Access Control** policies and configure the following policies and their **Policy Setting**.

Option	Action
User Account Control: Behavior of the elevation prompt for administration in Admin Approval Mode	Elevate without prompting.
User Account Control: Detect application installations and prompt for elevation	Disabled.
User Account Control: Run all administrators in Admin Approval Mode	Disabled.

8. Restart the domain controller machine to apply the changes.

What to do next

Install the VCM Windows Agent on licensed Windows machines in your environment, and then re-enable the group policy on the domain controller. See "Install the VCM Windows Agent on Your Windows Machines" on page 83.

Install the VCM Windows Agent on Your Windows Machines

Install the VCM Windows Agent on each Windows machine to manage.

Before you can collect data from Windows machines, you must install the VCM Windows Agent on the licensed Windows machines in your environment to enable communication between the Collector and the target machines.

You can use VCM to install the Agent or you can install the Agent manually. When you install a VCM Collector, the VCM Windows Agent is automatically installed. The Collector Agent is locked and cannot be unlocked, uninstalled, or upgraded.

Prerequisites

- License the Windows machines on which you install the Agent. See "License Windows Machines" on page 80.
- Disable UAC before you install the Agent on Windows 7, 2008, 2008 R2, or Vista machines. See "Disable User Account Control for VCM Agent Installation" on page 81.

Procedure

1. Click **Administration**.
2. Select **Machines Manager > Licensed Machines > Licensed Windows Machines**.
3. In the data grid, select one or more Windows machines on which to install the Agent and click **Install**.
4. On the Machines page, verify that the target machines appear in the Selected list and click **Next**.
5. On the Install Options page, select the installation options and click **Next**.

Option	Description
Share	Location to install the Agent. The default location is `ADMIN$`.
Path	Path for the Agent files. The default path includes `CMAgent`.
Install From	VCM Collector from which to install the Agent.
DCOM	Communication protocol for the Agent. The default setting is DCOM.
HTTP	Secure communication protocol for the Agent. Use HTTP, which installs the HTTP Listener on the target machine and configures it to listen on the designated port.
Port	Designated port for the HTTP Listener.
Install using a proxy server	For Windows Proxies and Windows Agents only. If the target machine is separated from the Collector by a proxy server, this option instructs the installation process to check for available proxy servers.

Option	Description
Lock the machine after installation	Ensures that VCM will not uninstall the Agent or replace it with a different version.
Reinstall Agent	Overwrites an installed Agent.

6. On the Schedule page, select **Run Action now** and click **Next**.

   You can schedule subsequent Agent installations to run later.

7. On the Important page, review the summary information and click **Finish**.

What to do next

- Verify that jobs have finished running. Click **Administration** and select **Job Manager > History > Other Jobs > Past 24 Hours**.
- Enable UAC on the Windows 7, 2008, 2008 R2, or Vista machines in your environment. See "Enable UAC After VCM Agent Installation" on page 89.
- Collect Windows data from VCM managed machines in your environment. See "Collect Windows Data" on page 90.

Locate the Enterprise Certificate

Locate the Enterprise Certificate before you install the VCM Agent on the managed Windows machine. VCM must access the Enterprise Certificate during the Agent installation.

If your Collector is operating in a full Public Key Infrastructure (PKI), and the target machine can validate the Collector root certificate (Enterprise Certificate), the `.pem` file is not required.

Procedure

1. Locate the Enterprise Certificate `.pem` file in the Collector's `c:\Program Files (x86)\VMware\VCM\CollecorData` folder.
2. Navigate to the Collector data directory at `c:\Program Files (x86)\VMware\VCM\CollectorData`.
3. If the certificate files are not in the default location, you must confirm the path to the files.
   a. Click **Administration**.
   b. Select **Settings > General Settings > Collector**.
   c. Select **Root directory for all collector files**.
   d. Confirm the file path in the **Value** column.

Manually Install the VCM Windows Agent

You can manually install the Windows Agent on the VCM managed machine by using the executable (EXE) file or the Microsoft Installer (MSI) file that is supplied with VCM.

- You use the EXE file to install the Agent in unattended, silent mode. EXE files detect an existing software version and provide the option to uninstall the existing version.
- You use the MSI file to install the Agent in unattended, silent mode. MSI files are database files. The Windows `msiexec.exe` executable file reads the data in the MSI file, and then installs the Agent.

  The MSI file uninstalls any existing, non-MSI Agent without sending a request. If you run the MSI installer again, the removal option is available.

  If you use a new MSI file to upgrade an MSI-installed Agent, the old Agent is uninstalled.

The VCM Enterprise Certificate was installed when you initially installed VCM. During the Agent installation process, if you select HTTP, VCM installs the Enterprise Certificate in the certificate store on the VCM managed machine.

The Collector root certificate authenticates Collector requests on the managed machine before it processes a collection or change request. The authentication process uses the Collector Certificate and established trust to the Enterprise Certificate.

Use the EXE File to Install the Agent

You can use the `EXE` file to manually install the VCM Windows Agent on a target machine. The directories in this procedure are default locations.

CAUTION **For Vista, Windows 7, and Windows 2008 only:** If you set the compatibility mode on an Agent executable file to a previous version of Windows, VCM might report the compatible operating system instead of the actual operating system. For example, on a Windows 7 machine, if you set the Agent to run in compatibility mode for Windows XP, the Agent will report that the machine is a Windows XP machine.

Prerequisites

Locate the Enterprise Certificate before you install the VCM Agent. See "Locate the Enterprise Certificate" on page 84.

Procedure

1. On your VCM Collector, open Windows Explorer and navigate to the Agent files directory at `C:\Program Files (x86)\VMware\VCM\AgentFiles`.
2. Copy the `CMAgentInstall.exe` file from the Collector to the target machine or a shared network location.

   The `CMAgentInstall.exe` file is located in the path relative to the installed software on the Collector.
3. On the target machine, use Windows Explorer and run the installation in either normal or silent mode.
   - For normal mode, run `CMAgentInstall.exe`.
   - For silent mode, run `CMAgentInstall.exe /s INSTALLPATH=%Systemroot%\CMAgent PORTNUMBER=26542 CERTIFICATEFILE=<filename>`.

   The `%Systemroot%` environment variable specifies the directory where Windows is installed, which is typically `\WINNT` or `\WINDOWS`.

   Use the following options for the installation.

Option	Action
`CMAgentInstall.exe`	Executable file used to install the Agent.

Option	Action
/s	Indicates a silent install. When you run CMAgentInstall.exe from the command line, VMware recommends that you install the Agent in silent mode. You must unlock the Agent before you can proceed with the installation. To unlock the Agent, use the -UNLOCK option. The syntax is: CMAgentInstall.exe /s -UNLOCK INSTALLPATH=%Systemroot%\CMAgent PORTNUMBER=26542 CERTIFICATEFILE=<filename> To relock your managed machine, you must submit a lock request from the VCM Collector. To submit the lock request, click **Administration** and select **Settings > General Settings > Installer**. Edit the **Lock Agent after it is installed?** setting to lock the managed machine.
INSTALLPATH	Location to install the Agent files.
PORTNUMBER	Used for HTTP Agents. If you do not include the PORT parameter, VCM uses DCOM and does not install the communication socket listener service. The certificate is not required.
CERTIFICATEFILE	Indicates the certificate that you generated or specified on the Collector during the Collector installation. The location of the certificate file is in the path relative to the installed software on the Collector. By default the path is C:\Program Files (x86)\VMware\VCM\CollectorData\[certificate name].pem. If you include PORTNUMBER, but do not use a certificate, you must use the CERTIFICATEFILE=SKIP parameter to allow an HTTP Agent to operate without a valid CERTIFICATEFILE path.

4. On the target machine, in Windows Explorer run CMAgentInstall.exe.

What to do next

- To confirm that the job finished running, click **Administration** and select **Job Manager > History > Other Jobs > Past 24 Hours**.
- Collect Windows data from VCM managed machines. See "Collect Windows Data" on page 90.
- Enable UAC on the Windows 7, 2008, 2008 R2, or Vista machines in your environment. See "Enable UAC After VCM Agent Installation" on page 89.

Use the MSI File to Install the Agent

You can use the MSI file to manually install the VCM Windows Agent on a target machine. The directories specified in this procedure are default locations.

Prerequisites

Locate the Enterprise Certificate before you install the VCM Agent. See "Locate the Enterprise Certificate" on page 84.

Procedure

1. On your VCM Collector, open Windows Explorer and navigate to the Agent files directory at `c:\Program Files (x86)\VMware\VCM\AgentFiles`.
2. Copy the `CMAgent[version].msi` file to the target machine or a shared network location.

   The `CMAgent[version].msi` file is located in the path relative to the installed software on the Collector.
3. Locate the `CMAgent[Version].msi` file.
4. If the file does not exist, you must copy `CMAgent[Version].msi` to the target machine, or install it from a network share onto the target machine.
5. Copy the Enterprise Certificate `.pem` file to the target machine.
6. On the target machine, in Windows Explorer, run `CMAgent[Version].msi` using the following syntax:

   ```
   msiexec /Option <Required Parameter> [Optional Parameter]
   ```

   For example:
   ```
   msiexec.exe /qn /i "[PathToFile]\CMAgent[Version].msi" [PORTNUMBER=<available port>] [INSTALLDIR="<new path>"]
   ```

   Use the following options for the installation.

Option	Action
`CMAgent[Version].msi`	When used with default options, this command removes any existing Windows Agent, installs the new Agent in the `%SystemRoot%\CMAgent` directory, and uses DCOM for communication. When you include an option with `CMAgent[Version].msi`, you must follow these conventions: ■ Include optional parameters in any combination and order. ■ After the required `/i` parameter, use uppercase letters for optional parameters. ■ Use quotation marks when a path includes spaces in the source file location and the `INSTALLDIR` parameter. To see details about the options, select **Start > Run > msiexec**.
`%Systemroot%`	Environment variable that specifies the directory where Windows is installed, which is typically `\WINNT` or `\WINDOWS`.
`/qb`	Runs the command in a basic user interface and displays the progress and error messages.
`/qn`	Runs the command in quiet mode without user interaction.
`/i`	Runs the command as an installation.
`/x`	Runs the command as an uninstall process.
`PORTNUMBER`	Installs the Windows Agent on the port number specified, and uses HTTP instead of DCOM. For HTTP installations where

Option	Action
	you include PORTNUMBER, you must include an Enterprise Certificate by using the following syntax: CERTIFICATEFILE="<drive>:\[mypath]\[mycert].pem" For example: msiexec.exe /qn /i "C:\temp\CMAgent[VersionNumber].msi" PORTNUMBER=2666 CERTIFICATEFILE="x:\mypath\mycert.pem" If you include PORTNUMBER, you must either include the path to the certificate file, or supplement the CERTIFICATEFILE parameter with the SKIP parameter .
INSTALLDIR	Location to install the Agent. Use to change the default root directory specification, which is %SystemRoot%\CMAgent. For example: msiexec.exe /qn /i "C:\temp\CMAgent[VersionNumber].msi" INSTALLDIR="C:\VCM"
CERTIFICATEFILE	Includes the Enterprise Certificate with either the path or the SKIP parameter. For example: CERTIFICATEFILE="x:\[mypath]\[mycert].pem" or CERTIFICATEFILE="SKIP"

What to do next

- To confirm that the job finished running, click **Administration** and select **Job Manager > History > Other Jobs > Past 24 Hours**.
- Collect Windows data from VCM managed machines. See "Collect Windows Data" on page 90.
- Enable UAC on the Windows 7, 2008, 2008 R2, or Vista machines in your environment. See "Enable UAC After VCM Agent Installation" on page 89.

Manually Uninstall the VCM Windows Agent

When you no longer manage a Windows machine with VCM, you uninstall the Agent from that target machine. If you used VCM to install the Agent, you must use VCM to uninstall the Agent.

After you remove the Windows Agent and remove the managed Windows machine from the list of licensed machines, VCM no longer manages the Windows machine and you can no longer collect data from it. To keep historical data, do not remove the Windows machine from VCM.

To remove the Windows machine, click **Administration** and select **Machines Manager > Licensed Machines > Licensed Windows Machines**.

The Windows Agent uninstall executable file exists on the VCM managed machine if you installed the Agent manually using CMAgentInstall.exe or CMAgentInstall.msi. Use this manual process to uninstall the Agent only if you used either of these commands to install the Agent.

Procedure

1. On the VCM managed machine, run `%SystemRoot%\CMAgent\Uninstall\Packages\CMAgentInstall\UnCMAgentInstall.exe`.

   This path displays the default location. The EXE file is located in the path relative to the installed software on the Collector.

Enable UAC After VCM Agent Installation

Enable User Account Control (UAC) on Windows 7, 2008, 2008 R2, and Vista machines after you install the VCM Agent.

You can enable UAC on a single Windows machine or a group of Windows machines.

- "Enable User Account Control on a Single Windows Machine" on page 89
- "Enable UAC By Using a Group Policy" on page 89

Enable User Account Control on a Single Windows Machine

You must enable User Account Control (UAC) on Windows 7, 2008, 2008 R2, or Vista machines after you install the VCM Agent on the target machines.

This procedure enables UAC on a Windows 2008 machine.

Procedure

1. On the target Windows 2008 machine, click **Start > Run**.
2. In the Run dialog box, type **msconfig** and click **OK**.
3. In the User Account Control dialog box, click **Continue**.
4. In the System Configuration dialog box, click the **Tools** tab.
5. In the Tool Name list, select **Enable UAC**.
6. Click **Launch**.
7. When the command is finished running, click **Close** and click **Close** again.
8. Restart the Windows 2008 machine to apply the changes.

What to do next

Collect data from managed Windows machines. See "Collect Windows Data" on page 90.

Enable UAC By Using a Group Policy

If you disabled the User Account Control (UAC) using a group policy, you can re-enable UAC VCM by using a group policy.

This procedure enables UAC on a Windows 2008 machine.

Procedure

1. On the Windows 2008 machine, click **Start > Run**.
2. In the **Run** dialog box, type **msconfig** and click **OK**.
3. In the User Account Control dialog box, click **Continue**.
4. In the **System Configuration** dialog box, click the **Tools** tab.
5. In the **Tool Name** list, select **Enable UAC**.

6. Click **Launch.**
7. When the command is finished running, click **Close** and click **Close** again.
8. Restart the Windows 2008 machine to apply the changes.

What to do next

Collect data from managed Windows machines. See "Collect Windows Data" on page 90.

Collect Windows Data

Start managing the Windows machines by performing an initial collection, which adds Windows machine data to VCM.

Use the default filter set to collect a general view of the Windows machines in your environment. The first time that you use the default filter to collect data, the Windows Agent returns all of the data specified in the filter and stores the data in the VCM database. All subsequent collections will return a delta against the data previously collected.

A delta collection includes only the differences between the data on the target machine and the data stored in the VCM database. If you need a full collection, you can specify that VCM collect all data again. A full collection can take a significant amount of time depending on the number of VCM managed Windows machines from which you are collecting.

When you perform a full collection from your entire environment, run the collection during non working hours so that users do not notice any performance impact on managed machines. After the initial collection is finished, subsequent delta collections will most likely not impact performance.

Prerequisites

- Collect the Accounts and Groups data types from the primary domain controller (PDC) in each domain to increase the performance of initial collections that require a SID lookup.
- To collect from Windows XP SP2 or Vista machines that use DCOM communication, you must enable ICMP pings in the firewall settings or disable ICMP pings in VCM.
- Verify that DCOM is enabled on the managed machine. Run `dcomcnfg` and select **Enable Distributed COM on this computer**.

Procedure

1. On the VCM toolbar, click **Collect**.
2. On the Collection Type page, select **Machine Data** and click **OK**.
3. On the Machines page, select the Windows machines from which to collect data and click **Next**.

   To move all visible Windows machines to the selection window, 500 at a time, use the double arrow.
4. On the Data Types page, select the **Select All** checkbox.
5. Select **Use default filters** and click **Next**.
6. On the Important page, resolve any conflicts and click **Finish**.

What to do next

- Verify that jobs have finished running. Click **Administration** and select **Job Manager > History > Other Jobs > Past 24 Hours**.
- Review the collection results. See "Windows Collection Results" on page 91.

Windows Collection Results

Continuous Windows machine management is based on the latest data you collect from target machines. You can view data and run actions, such as reports or compliance, based on the collected data.

Windows data appears in VCM and is available for several management actions, including Console dashboards and reports, Compliance views, and VCM Patching. The displayed data is only as current as the last time you collected the data.

Option	Description
Console	Displays dashboards and reports based on collected data. Use the Console to view data that is relevant to day-to-day operations, troubleshooting, and analysis. ■ To view the dashboards, click **Console** and select **Dashboards > Windows > Operating Systems**. ■ To view the summary reports, click **Console** and select **Windows > Operating System > Machines**. You can view the data in a summary report or data grid format.
Compliance	Determines if the data collected from VCM managed Windows machines meets specified compliance values, and allows you to run compliance remediation actions. ■ To run a compliance check, click **Compliance** and select **Machine Group Compliance**. ■ To create rule groups, rules, filters, and templates, see the online help.
Reports	Runs pre-configured reports or you can create custom reports. VCM runs reports against the latest collected data. Depending on the data volume or complexity of the requested report, it might take time to generate the report. For information to schedule and disseminate reports, see the online help. ■ To use the reporting options, click **Reports** and select **Machine Group Reports > Windows**.
Patching	Assesses target machines to determine if the patching status of the Windows machines is up-to-date. You can install the latest patches on target machines. ■ To assess and patch Windows machines, click **Patching** and select **Windows**. ■ To run assessments and patch your Windows machines, see the online help.

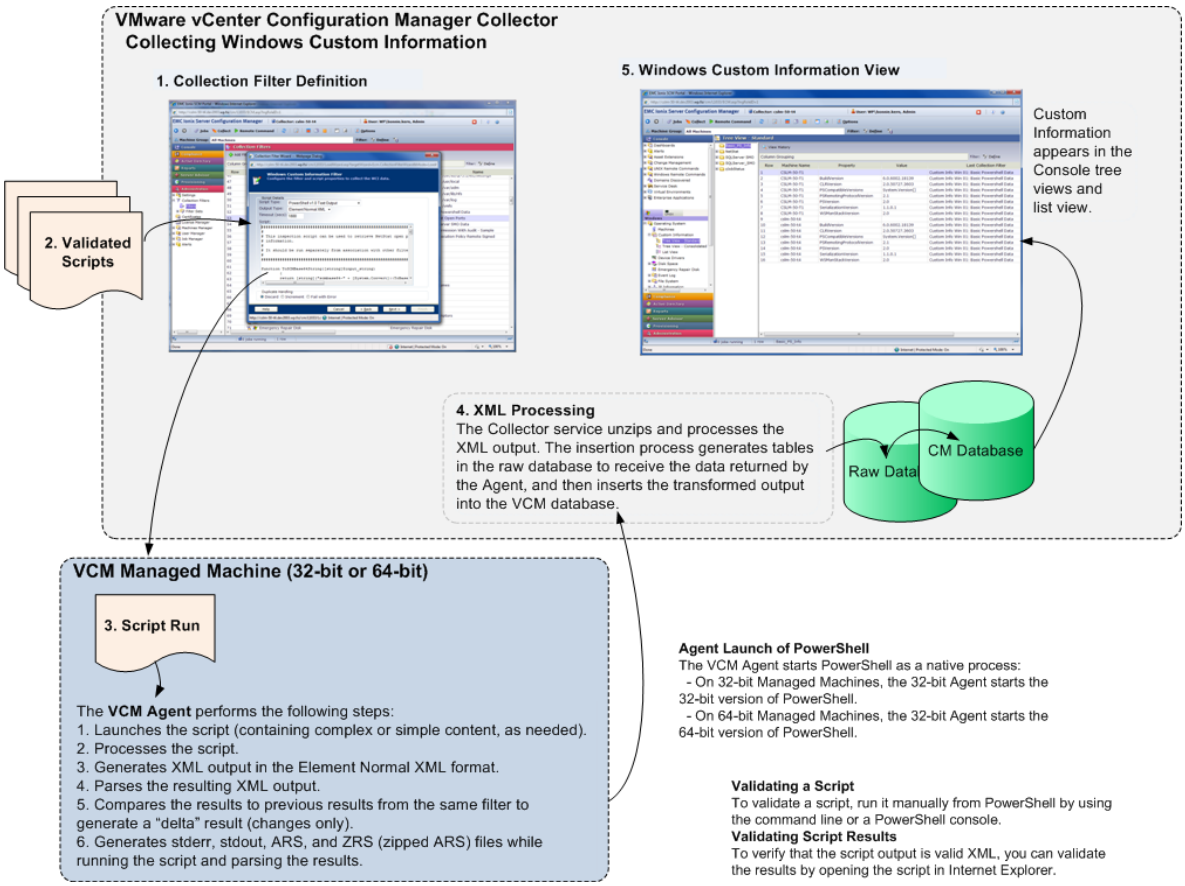
After the initial discovery is finished, perform a weekly discovery to update the list of available Windows machines. To schedule a VCM discovery job, click **Administration**, select **Job Manager > Scheduled**, and follow the wizard.

Getting Started with Windows Custom Information

Windows Custom Information (WCI) is data collected from VCM managed machines that is created by PowerShell scripts. WCI supplements and extends the data collected by VCM from managed Windows machines using other VCM data types.

You can create or modify WCI scripts to collect almost any data type that is accessible from VCM managed machines. VCM supports PowerShell scripting and XML output to collect Windows Custom Information.

Figure 7–1. Windows Custom Information Collection Process


VMware vCenter Configuration Manager Collector
Collecting Windows Custom Information
1. Collection Filter Definition
2. Validated Scripts
5. Windows Custom Information View
Custom Information appears in the Console tree views and list view.
4. XML Processing
The Collector service unzips and processes the XML output. The insertion process generates tables in the raw database to receive the data returned by the Agent, and then inserts the transformed output into the VCM database.
Raw Data
CM Database
VCM Managed Machine (32-bit or 64-bit)
3. Script Run
The VCM Agent performs the following steps:
1. Launches the script (containing complex or simple content, as needed).
2. Processes the script.
3. Generates XML output in the Element Normal XML format.
4. Parses the resulting XML output.
5. Compares the results to previous results from the same filter to generate a "delta" result (changes only).
6. Generates stderr, stdout, ARS, and ZRS (zipped ARS) files while running the script and parsing the results.
Agent Launch of PowerShell
The VCM Agent starts PowerShell as a native process:
- On 32-bit Managed Machines, the 32-bit Agent starts the 32-bit version of PowerShell.
- On 64-bit Managed Machines, the 32-bit Agent starts the 64-bit version of PowerShell.
Validating a Script
To validate a script, run it manually from PowerShell by using the command line or a PowerShell console.
Validating Script Results
To verify that the script output is valid XML, you can validate the results by opening the script in Internet Explorer.

To get started collecting Windows Custom Information, you have prerequisites and steps to perform to create and validate your PowerShell script.

Procedure

1. "Prerequisites to Collect Windows Custom Information" on page 93

   To collect Windows Custom Information from VCM managed machines, you have several prerequisites.

2. "Collecting Windows Custom Information" on page 104

To collect Windows Custom Information (WCI) using script-based filters, you must do the following tasks:

- Create and verify your custom PowerShell script.
- Install PowerShell on the VCM managed machines to be used for WCI collections.
- Use VCM to collect WCI data from the managed machines using your script-based filter.

You can view the job status details and collection results, and run reports on the collected data.

Prerequisites to Collect Windows Custom Information

To collect Windows Custom Information from VCM managed machines, you have several prerequisites.

Prerequisites

- Understand how to write and run PowerShell scripts. See "References on PowerShell and Script Signing" on page 98 or the Windows PowerShell online help.
- Write your own PowerShell script to return data in a VCM compatible, element-normal XML format, or obtain PowerShell scripts from VMware Professional Services or another source. See "Using PowerShell Scripts for WCI Collections" on page 93.
- Make sure that your PowerShell script is accessible when you paste the script content into the Script area of the collection filter on the VCM Collector.
- Confirm that the VCM Collector includes PowerShell 2.0 if the Collector is a client for WCI collections.
- Confirm that PowerShell 2.0 is installed on each VCM managed machine that will be used for WCI collections. See "Install PowerShell" on page 106.
- Upgrade older VCM Agents on the VCM managed machines from which you collect Windows Custom Information, and then install the VCM 5.3 Agent or later on these machines.
- Understand the script signing policies if you use PowerShell 2.0. See "PowerShell Script Signing Policies" on page 97.
- Set the PowerShell execution policy on the VCM managed machine. See "Built-in PowerShell Policy Settings" on page 98.
- Understand how VCM manages Windows Custom Information data changes. See "Windows Custom Information Change Management" on page 103.
- Confirm or update the Agent Thread Administration settings on the VCM Collector. The default value is set to below normal thread priority, and the Agent Data Retention default is set to a 15-day change log. See the online help.

Using PowerShell Scripts for WCI Collections

Windows Custom Information (WCI) uses PowerShell as the scripting engine and the element-normal XML format as the output that is inserted into the VCM database.

WCI supports PowerShell 2.0 and works with later versions of PowerShell.

- PowerShell 2.0 is the base requirement for WCI in VCM because of its ability to set the execution policy at the process level.
- You can run WCI PowerShell collection scripts against Windows machines that have PowerShell 1.0 installed, although this usage is not supported or tested. If the collection scripts do not use PowerShell 2.0 commands, your WCI filters that use the in-line method to pass a WCI script to PowerShell will operate correctly.

The WCI data type uses extensions to the VCM Windows Agent. The extensions allow the Agent to invoke PowerShell scripts. Using the script-based collection filter, VCM passes the PowerShell scripts to a VCM managed machine, and the VCM Agent parses the resulting XML output. The default WCI filter returns the PowerShell version information from the managed machines.

WCI data type extensions are flexible because they use filter parameters that the command line uses to invoke the scripting engine. The WCI extensions use a COM class name to specify the parser required for the Agent to parse the script output, and allow new types of parsers to be added at the Agent. This approach extends the support of multiple scripting engines, languages, and output formats.

Guidelines in PowerShell Scripting for WCI

When you develop custom PowerShell scripts to collect the Windows Custom Information (WCI) data type from VCM managed Windows machines, follow these guidelines.

- Make XML element names unique at the same level.

  For example, you can specify two child nodes that are not siblings.

- Make attributes unique at the same level.
- Use unique XML element names to generate valid VCM XML. The XML elements are code blocks that include the element's start and end tags. The element can contain other elements, text, attributes, or a combination of them.
- Use repeatable identifiers to prevent false indications of changes at the Collector. If your element labels (identifiers) are not the same for every collection of the same item, you will see false additions, changes, and deletions in the VCM change log.
- Confirm that the script returns valid XML element names and attribute names.

  If the data to be returned is an element name or an attribute name that is not valid for XML, you can encode the name using the [`ToCMBase64String`] function. A VCM Collector job, called the inserter, is executed during each collection. The inserter recognizes the names that are encoded with this function and decodes them in the raw insertion process.

  The inserter parses the resulting XML file and inserts the data into a new raw database table named VCM_Raw by default. The XML process transforms the raw data into data that appears in VCM.

  The function is defined as follows.

  ```
  function ToCMBase64String([string]$input_string)
  {
  return [string]("cmbase64-" +
  [System.Convert]::ToBase64String([System.Text.Encoding]::UNICODE.GetBytes
  ($input_string))).replace("=","-")
  }
  ```

- Include a comment block and configurable parameter entries near the start of the script so that when you clone a WCI collection filter you can see the parameters and set them when you edit the collection filter. To view and edit the collection filters, click **Administration** and select **Collection Filters > Filters**.
- Redirect any variable declarations in the script to out-null, along with any other tasks that generate output that is not part of the XML result set. For example, you can use the following command.

  ```
  [reflection.assembly]::LoadWithPartialName("Microsoft.SqlServer.Smo") > out-
  null
  ```

- Do not include any formatting, white space, carriage returns, or line feeds at the end of elements, nodes, or attributes.

Challenges in PowerShell Scripting for WCI

When you develop custom collection scripts, understand the challenges that you might encounter while scripting in PowerShell to collect the Windows Custom Information (WCI) data type from VCM managed Windows machines.

PowerShell scripts can use the split method of PowerShell strings, which separates the columns of the rows into separate values in arrays. For example, Windows provides the `schtasks.exe` utility to manage scheduled tasks on a local or remote computer and report on the scheduled tasks.

The split method of PowerShell strings in the `$schtasks` script separates the columns of the `$schtasks` rows into separate values in arrays.

- Column names row provides the names to use for attributes.
- Corresponding data from the scheduled task rows provides the values to use for these attributes.

The top-level name of `<schtasks>` is an arbitrary name that you apply to distinguish the results of this script from other results. The XML script returns the parsed data, which resembles the following structure.

```
<schtasks>
     <taskname1>
          <attribute1>Value1</attribute1>
          <attribute2>Value2</attribute2>
     </taskname1>
     <taskname2>
          <attribute1>Value1</attribute1>
          <attribute2>Value2</attribute2>
     </taskname2>
</schtasks>
```

The returned data can include the following content, which causes problems.

- White space, such as tabs or spaces, is not allowed in returned data.
- Column names include spaces.
- Specific task entries do not include a unique and repeatable identifier.
- Values can contain XML syntax in functions, which you must enclose in CDATA.

Column Names Include Spaces

Running the `schtasks` command without any options displays a column name of `Next Run Time`. Because this name includes spaces, you cannot use it as an attribute name in an XML document. Running the `schtasks` command verbosely generates other column names that include spaces. Although you cannot use these invalid names as attribute names, you can preserve the names by using VCM encoding standards.

To preserve these column names in the form that `schtasks` returns and allow for XML handling, VCM encodes the column names with the `ToCMBase64String` function. To create a valid XML form of an element name or attribute name, this function uses Unicode Base64 encoding and character substitution, such as using a dash instead of an equal sign, as shown in the following example.

```
function ToCMBase64String([string]$input_string)
     {
     return [string]("cmbase64-" +
     [System.Convert]::ToBase64String([System.Text.Encoding]::
     UNICODE.GetBytes($input_string))).replace("=","-")
     }
```

Using this function corrects the invalid column name data.

VCM prefaces the string with `cmbase64-` so that the VCM inserter can decode the data and load the decoded data into the VCM database.

The valid XML appears as follows.

```
<cmbase64-TgBlAHgAdAAgAFIAdQBuACAAVABpAG0AZQA->
12:32:00, 5/26/2010
</cmbase64-TgBlAHgAdAAgAFIAdQBuACAAVABpAG0AZQA->
```

Invalid XML omits the encoding function as follows.

```
<Next Run Time>
12:32:00, 5/26/2010
</Next Run Time>
```

Task Entries Do Not Include a Unique and Repeatable Identifier

Use repeatable identifiers to prevent false indications of changes at the Collector. If your element labels (identifiers) are not the same for every collection of the same item, you will see false additions, changes, and deletions in the VCM change log.

The Windows `schtasks` command does not include a unique and repeatable identifier for specific task entries. Because unique element names are a requirement for valid VCM XML and repeatable identifiers help prevent false indications of changes at the VCM Collector, you must code the task names correctly in your script.

To create unique and repeatable element names, one method is to create a task entry name based on a hash of the data in the row. You can use this method for data that does not have a name-type attribute, where the task name exists but is not guaranteed to be unique. When the task name is user-friendly and useful, you must attempt to preserve the name and use it in the collection script.

To preserve the user-friendly name, use the task name as the element name for the task rows. When you create a collection filter that uses your script, you must select the incremental duplicate handling option so that the collection process includes an incremental entry in the list of entries where the same task name appears multiple times.

For example, in a sample test environment, many Windows machines had more than one task named `GoogleUpdateTaskMachineCore`. A PowerShell script can label the rows as Task1, Task2, and so on. If you delete Task1, Task2 becomes Task1, and VCM displays multiple change details for Task1, such as the command line and the next run time. This report would be incorrect because even though Task 1 would have changed place in the sequence, the task would not have changed.

The task names are labeled accordingly.

- The first task entry is `GoogleUpdateTaskMachineCore`.
- The second task entry is labeled `GoogleUpdateTaskMachineCore_1`.

Because task names can contain characters that are not valid in XML element names, VCM encodes the task names with the `ToCMBase64String` function. If you reorder the list of tasks whose names are identical, VCM can still report extra changes. For this reason, require the VCM user interface to display the friendly task names.

Enclose Values that Can Contain XML Syntax in CDATA

When you develop your custom PowerShell scripts to collect the Windows Custom Information data type from VCM managed Windows machines, you must use CDATA to enclose values that contain XML syntax.

For example:

```
function wrapInCDATA( [string]$input_string)
{
[string]$wrappedInCDATA | out-null
if ( $input_string.Length -gt 0 )
{
$wrappedInCDATA = ("<!" + "[CDATA" + "[" + $input_string + ("]" + "]" + ">")
)
}
return $wrappedInCDATA
}
```

PowerShell Script Signing Policies

With PowerShell 2.0 you can set the script signing policies at the machine, user, and process levels. The process level runs a single execution of `powershell.exe`.

In VCM, Windows Custom Information (WCI) uses script type information in the collection filter to determine how to execute PowerShell and how to pass the script to it.

Use the following methods to pass a WCI script to PowerShell.

- **In-line:** The default WCI filter uses an in-line script to collect basic information about the PowerShell version, .NET version, and execution policy settings. The in-line option requires a collection script that is represented as a single line of PowerShell code. Because the filter runs an in-line script on the PowerShell command line, instead of using a file, the execution policy does not apply.
- **Script file:** For script-based filters in WCI, the default script type command line includes options to set the process-level execution policy to Remote Signed. The script requires that the execution policy be set to Remote Signed at the most restrictive level because the script runs from a file that resides locally on the VCM managed Windows machine. For WCI, VCM can execute collection scripts on managed machines where the machine and user level signing policies are set to any level, without requiring you to change the setting.

Built-in PowerShell Policy Settings

Before you use the WCI collection filter to run file-based PowerShell scripts on the VCM Collector and your VCM managed machines, you must change the execution policy on the VCM managed machines.

PowerShell contains built-in execution policies that limit its use as an attack vector. By default, the execution policy is set to Restricted, which is the primary policy for script execution.

The following policy settings apply to PowerShell scripts.

- **AllSigned:** PowerShell scripts must be signed by a verifiable certificate from the Software Publishing Certificate store. The typical file extension is `.ps1`. For signed scripts, you can set the execution policy to **All Signed**. You must sign the scripts and distribute the appropriate certificates before you collect WCI data.
- **RemoteSigned:** A verifiable certificate must sign any PowerShell script that you download from the Internet using a supported browser such as Internet Explorer. Script files that are not required to be signed are scripts that you create locally or scripts that you download using a method that does not support flagging the file source. For un-signed scripts, you must set the execution policy to the most restrictive level of **Remote Signed**. You can set the policy directly by using a Group Policy Object (GPO) with a VCM remote command. You can use a registry change action or enforceable compliance. For example:

  ```
  HKLM\Software\Microsoft\PowerShell\1\ShellIds\Microsoft.PowerShell
  "ExecutionPolicy"="RemoteSigned"
  ```

- **Unrestricted:** All PowerShell script files run regardless of whether they are signed by a verifiable certificate.
- **Restricted:** You can use PowerShell interactively or to run commands directly from the command line. This setting is the default.

References on PowerShell and Script Signing

For information about Windows PowerShell and script signing policies, see the Microsoft Web site.

Create an Example PowerShell Script for Scheduled Tasks

Use a custom PowerShell script to collect Windows Custom Information (WCI) data from VCM managed Windows machines. With this example, you can learn how to use PowerShell scripts to collect WCI data for scheduled tasks.

Windows provides the `schtasks.exe` utility to report on scheduled tasks that you create in the Task Scheduler user interface or by using the `AT` command. The `schtasks.exe` utility enables you to manage scheduled tasks on a local or remote computer and to report on the scheduled tasks.

The `schtasks` command returns basic information about scheduled tasks. The data returned by `schtasks` includes multiple rows. PowerShell structures the `$schtasks` variable in an array. For example, `$schtasks[0]` represents the first row. To view the result set, use `$schtasks[n]`, which displays the following status:

- `$schtasks[0]` is blank.
- `$schtasks[1]` contains column names.
- `$schtasks[2]` is the first row of task data.

Prerequisites

- Review the guidelines to create PowerShell scripts for WCI collections, and understand the challenges in PowerShell scripting. See "Guidelines in PowerShell Scripting for WCI" on page 94.
- Understand how to write and run PowerShell scripts. See "References on PowerShell and Script Signing" on page 98 or the Windows PowerShell online help.

Procedure

1. On your VCM managed Windows machine, click **Start**.
2. Select **All Programs > Accessories > Windows PowerShell**.
   - On a 64-bit Windows machine, select **Windows PowerShell (x86)** to run the 32-bit version of PowerShell.
   - On a 32-bit Windows machine, select **Windows PowerShell**.
3. Run the command to set the source of data for the collection script.

   ```
   $schtasks = schtasks /query /v /fo:csv
   ```

   The following options are available.

Option	Description
`/query /v`	Displays additional information about scheduled tasks. Be aware that verbose formatting is difficult for automated processing.
`schtasks /query /v /fo:csv`	Displays verbose task output and sets the source of data for the collection script to a comma-separated value (csv) result set.
`schtasks /query /?`	Displays additional command options.

4. To return the data to the VCM Collector, parse the data into a structure that is compatible with the VCM XML format. The sample script parses the data as shown in the following code.

   ```
   ##############################################################################
   ##
   #
   # This inspection script can be used to retrieve scheduled tasks
   information
   # for tasks created through the Scheduler UI or through the AT command.
   #
   ```

```
##############################################################################-
##
function ToCMBase64String([string]$input_string)
     {
return [string]("cmbase64-" +
[System.Convert]::ToBase64String([System.Text.Encoding]::UNICODE.GetBytes
($input_string))).replace("=","-")
     }
##############################################################################-
##
[string]$cihash | out-null
#create a hashtable to check for duplicate rows
$hasharray = @{}
$clTasks = ("<Scheduled_Tasks>")
$split = [char]3
$schtasks = schtasks /query /v /fo:csv
if ($schtasks.count -gt 1)
     {
     #depending on OS, the first row may be blank
     #use $k to determine whether to start at the first or second row
     if ($schtasks[0] -eq "")
          {
          $k = 1
          }
     else
          {
          $k = 0
          }
     $cols = $schtasks[$k].substring(1,$schtasks[$k].length-
     2).replace("""","""",$split).split($split)
     #find the HostName and TaskName columns
     $hostcol = -1
     $namecol = -1
     $j = 0
     while (($j -lt $cols.count) -and (($hostcol -eq -1) -or ($namecol -eq
     -1)))
          {
```

```
     if (([string]$cols[$j]).toupper() -eq "HOSTNAME")
          {
          $hostcol = $j++
          }
          else
               {
               if (([string]$cols[$j]).toupper() -eq "TASKNAME")
                    {
                    $namecol = $j++
                    }
               else
                    {
                    $j++
                    }
               }
     }
#save first column name, to check for repeated column rows
$firstcol = $cols[0]
#encode each column name
for ($j=0;$j -lt $cols.count;$j++)
     {
     $cols[$j] = [string](ToCMBase64String($cols[$j]))
     }
#loop through each row
#start at $k+1, because the first row may blank, and the first
populated row is column names
for ($i=$k+1;$i -lt $schtasks.count;$i++)
     {
     #make sure this is a data row
     $row = ([string]($schtasks[$i])).trim()
     if ($row.contains("""","""))
          {
          #split the row
          $task = $schtasks[$i].substring(1,$schtasks[$i].length-
          2).replace("""","""",$split).split($split)
```

```
#some operating systems will return columns multiple times
in the result set
if ($task[0] -ne $firstcol)
     {
     #if we did not find a TaskName column, just tag each
     row as Task-n
     if ($namecol -gt -1)
          {
          $clTasks += "<" +
          [string](ToCMBase64String($task[$namecol])) + ">"
          }
     else
          {
          $clTasks += ("<Task-" + ([string]($i-1)) + ">")
          }
     for ($j=0;$j -lt $task.count;$j++)
          {
          #skip the hostname field, since we are doing a
          local inspection
          if (-not($j -eq $hostcol))
               {
               $clTasks += ("<" + $cols[$j] + ">")
               $clTasks += $task[$j]
               $clTasks += ("</" + $cols[$j] + ">")
               }
          }
     #if we did not find a TaskName column, just tag each
     row as Task-n
     if ($namecol -gt -1)
          {
          $clTasks += "</" +
          [string](ToCMBase64String($task[$namecol])) + ">"
          }
     else
          {
          $clTasks += ("</Task-" + ([string]($i-1)) + ">")
          }
```

```
                        } #end data row that is not columns repeated
                    } #end data row
                } #end row loop
            }

    $clTasks += ("</Scheduled_Tasks>")
    write-host $clTasks
```

What to do next

Develop your own custom PowerShell script. See "Create Your Own WCI PowerShell Collection Script" on page 105.

After you generate your PowerShell script, do the following:

1. Build a collection filter in VCM.
2. Paste the content of your script into the collection filter.
3. Collect data using the script-based collection filter.

   To view the collected WCI data in VCM, click **Console** and select **Windows Operating System > Custom Information > List View**.

Windows Custom Information Change Management

VCM manages Windows Custom Information (WCI) data changes on a per-filter basis on VCM managed Windows machines. When multiple filters return data using the same top-level XML element name, each filter applies unique change detection.

When you use multiple collection filters to collect WCI data, follow these guidelines.

- Create filters that collect data in a parallel manner. When you use filters in an unparallel way, every time the file system updates to add a new file or remove an existing file, both filters generate "new file" and "deleted file" events, which causes overlap of the data. See the following examples.
  - Use one filter to collect data from `C:\` and another filter to collect data from `C:\Windows`.
  - Use a separate filter to collect data from `C:\Windows` with audit information, and another filter to collect data from `C:\Windows` without audit information.
- Use only one filter to collect data from NetStat.
- Use multiple filters to collect data from the NTFS file system.

  For example, use one filter to collect data in `C:\`, and another filter to collect data in `C:\Windows\System`. These collections merge under the top-level element `NTFSDirectory` without overlap, because each filter collects separate parts of the file structure and avoids extra change reporting.
- Do not create filters that overlap collected WCI data. Overlap can occur if you use filters that do not collect data in a parallel manner. See the following guidelines.
- Do not use multiple filters to collect the same data for NetStat Open Ports.

  When the filters return data under the top-level element name, and a managed machine starts to listen on port 80, each filter initially reports the data as a newly created value. This action causes overlap of

- Do not create two filters to collect data on the File Permission With Audit data type from different parts of a managed machine's file system.

Collecting Windows Custom Information

To collect Windows Custom Information (WCI) using script-based filters, you must do the following tasks:

- Create and verify your custom PowerShell script.
- Install PowerShell on the VCM managed machines to be used for WCI collections.
- Use VCM to collect WCI data from the managed machines using your script-based filter.

You can view the job status details and collection results, and run reports on the collected data.

Procedure

1. "Create Your Own WCI PowerShell Collection Script" on page 105

   Create or modify your Windows Custom Information (WCI) scripts to collect almost any data type that is accessible from VCM managed Windows machines. To return data in a VCM compatible, element-normal XML format, you create your own PowerShell script or obtain PowerShell scripts from VMware Professional Services or another source and modify them for your own collections.

2. "Verify that Your Custom PowerShell Script is Valid" on page 105

   Verify that your PowerShell script adheres to valid XML before you use the script to collect Windows Custom Information (WCI) from VCM managed machines.

3. "Install PowerShell" on page 106

   Verify that PowerShell 2.0 is installed on each VCM managed Windows machine used to collect Windows Custom Information (WCI).

4. "Collect Windows Custom Information Data" on page 106

   Use the Windows Custom Information (WCI) data type to perform user-defined, script-based collections on your VCM managed machines. To collect the custom data, you build a collection filter that includes a script with parameters to run the script and process the results.

5. "View Windows Custom Information Job Status Details" on page 108

   When you run Windows Custom Information (WCI) collection filter scripts, VCM captures detailed information and displays status about exit codes and standard error output for each job that processed the script or filter. You can view the job status details in Job Manager.

6. "Windows Custom Information Collection Results" on page 109

   Examine the results of your Windows Custom Information (WCI) collected data in the VCM tree views and list view.

7. "Run Windows Custom Information Reports" on page 110

   Generate your own reports or run existing reports on Windows Custom Information (WCI) data that you collected using your custom PowerShell scripts.

8. "Troubleshooting Custom PowerShell Scripts" on page 111

   If you encounter problems when you run custom PowerShell scripts, run the script as a `.ps1` file and correct any errors before you use the script with a VCM collection filter.

Create Your Own WCI PowerShell Collection Script

Create or modify your Windows Custom Information (WCI) scripts to collect almost any data type that is accessible from VCM managed Windows machines. To return data in a VCM compatible, element-normal XML format, you create your own PowerShell script or obtain PowerShell scripts from VMware Professional Services or another source and modify them for your own collections.

WCI internally stores data in a hierarchy, so your collection script must provide the complete data structure in the standard tree view. The root element in the XML result data set becomes a top-level root element in the WCI data type node. Child elements appear in the same locations in VCM as the locations they populate in the XML document returned by the script.

Prerequisites

- Understand how to write and run PowerShell scripts. See "References on PowerShell and Script Signing" on page 98 or the Windows PowerShell online help.
- Plan your data structure to display WCI data in a tree hierarchy based on the data structure specified in the user-defined collection scripts. For an example, see Windows Custom Information Tree View - Standard in the online help.
- Review the guidelines to create PowerShell scripts for WCI collections and understand the challenges. See "Guidelines in PowerShell Scripting for WCI" on page 94.
- Review the example PowerShell script to see a sample script used for a WCI collection. See "Create an Example PowerShell Script for Scheduled Tasks" on page 98.

Procedure

1. On your VCM Collector or managed Windows machine, click **Start**.
2. Select **All Programs > Accessories > Windows PowerShell**.
   - On a 64-bit Windows machine, select **Windows PowerShell (x86)** to run the 32-bit version of PowerShell.
   - On a 32-bit Windows machine, select **Windows PowerShell**.
3. Create your PowerShell script and save it to the location of your choice.

What to do next

Verify that your PowerShell script adheres to valid XML before you can use the script to collect WCI data from VCM managed machines. See "Verify that Your Custom PowerShell Script is Valid" on page 105.

Verify that Your Custom PowerShell Script is Valid

Verify that your PowerShell script adheres to valid XML before you use the script to collect Windows Custom Information (WCI) from VCM managed machines.

To verify that your script is valid, run the script in PowerShell.

Procedure

1. On your VCM Collector or managed Windows machine, open a command prompt.
2. Run `powershell.exe` from the command line.
3. Paste your script into the PowerShell window.

   If your script does not run, press Enter.
4. Make sure that your script runs without errors.

   Errors appear in red in the PowerShell window.
5. If errors occur, resolve them before you proceed.

   A valid script returns a set of XML content without any formatting, white space, carriage returns, or line feeds at the end of elements, nodes, or attributes.

What to do next

Install PowerShell on your VCM managed machines. See "Install PowerShell" on page 106.

Install PowerShell

Verify that PowerShell 2.0 is installed on each VCM managed Windows machine used to collect Windows Custom Information (WCI). PowerShell 2.0 is supported on all platforms that support PowerShell 1.0.

- PowerShell is installed by default on Windows 2008 R2 and Windows 7 machines.
- For Windows XP, 2003, 2003 R2, 2008, and Vista machines, you must install PowerShell separately.
- You cannot install PowerShell on Windows 2000 or NT4 machines.

Because of its ability to set the execution policy at the process level, PowerShell 2.0 is the base requirement for WCI in VCM. If you run the standard WCI non-inline collection filters against PowerShell 1.0 VCM managed machines, the collection process will fail.

If PowerShell is not installed on the target VCM managed machine, the WCI collection returns a `Not Executed` status. See "View Windows Custom Information Job Status Details" on page 108.

What to do next

Reboot the VCM managed machine after you install or upgrade PowerShell to ensure that collections work properly.

Collect Windows Custom Information Data

Use the Windows Custom Information (WCI) data type to perform user-defined, script-based collections on your VCM managed machines. To collect the custom data, you build a collection filter that includes a script with parameters to run the script and process the results.

When you use the script-based filter in a collection, the VCM Agent calls a script engine to run the script, parse the results to return the collected data to the VCM database, and display the results in the VCM Console. During the collection process, the VCM Agent starts PowerShell, which runs the script and generates the XML result file. The Agent parses the XML result into a format that VCM can use to check for changes, and returns the changes to the Collector.

CAUTION Do not limit collections to deltas when you select a data type in the Collect wizard. If you limit collections to deltas, VCM purges all existing WCI data from the managed machine's master file and from the VCM database, and replaces the WCI data with newly collected data. You must select the option in the Collect wizard so that VCM does not purge WCI data during collections.

Prerequisites

You must perform several tasks. See "Prerequisites to Collect Windows Custom Information" on page 93.

Procedure

1. On your VCM Collector, click **Administration**.
2. Select **Collection Filters > Filters** and click **Add Filter**.
3. On the Name and Description page, type a name and description for the filter and click **Next**.
4. On the Data Type page, select **Windows**.
5. Select the **Custom Information (Win)** data type and click **Next**.
6. On the Windows Custom Information Filter page, select the options to add and configure the filter and click **Next**.

Option	Description
Script Type	Set the format of your PowerShell script to **PowerShell v2.0 Text Output**.
Output Type	Set the resulting output for your PowerShell script to **Element Normal XML**.
Timeout	Retain the default setting of `300` seconds to specify the amount of time the Agent allows a PowerShell script to run before it attempts to end the process. If the script takes more than 300 seconds to run on the VCM managed machine, increase the setting to `900`.
Script	Paste the content of your PowerShell script into the Script text pane. Your script contains statements that are specific to the data type to collect.
Duplicate Handling	Set the method to handle duplicates to **Increment** to resolve duplicate violations of duplicate path attributes in the PowerShell script.

7. On the Important page, review the summary information and click **Finish**.

What to do next

Run a script-based collection filter to collect WCI data using from VCM managed Windows machines. See "Run the Script-Based Collection Filter" on page 107.

Run the Script-Based Collection Filter

Use a collection filter and your PowerShell script to collect Windows Custom Information (WCI) from VCM managed Windows machines.

Procedure

1. On your VCM Collector, click **Collect**.
2. On the Collection Type page, select **Machine Data** and click **OK**.
3. On the Machines page, select the managed machines from which to collect WCI data and click **Next**.
4. Click **Select Data types to collect from these machines** and click **Next**.

   VCM runs a default collection filter for the data type you select.
5. Select **Do not limit collection to deltas** and click **Next**.

   VCM does not purge WCI data during the collection.
6. On the Data Types page, expand **Windows** and select **Custom Information (Windows)**.
7. Click **Select data filters** and click **Next**.
8. On the Filters page, select your WCI filter.
9. Click the arrow to move your filter to the selection area and click **Next**.
10. (Optional) On the Important page, select **View Selected Filter Details** to see details about your collection filter.
11. Click **Close** and click **Finish**.

What to do next

- To confirm that the job finished running, click **Administration** and select **Job Manager > History > Other Jobs > Past 24 Hours**.
- View the detailed status about exit codes and standard error output for each job that processed the script or filter. See "View Windows Custom Information Job Status Details" on page 108.

View Windows Custom Information Job Status Details

When you run Windows Custom Information (WCI) collection filter scripts, VCM captures detailed information and displays status about exit codes and standard error output for each job that processed the script or filter. You can view the job status details in Job Manager.

The following procedure displays data for an instant collection performed in the last 24 hours.

Prerequisites

- Verify that all prerequisite components exist on the VCM managed machine. If a prerequisite component such as PowerShell is not installed or available on the managed machine, the script cannot run and a status of `Not Executed` appears in the Status column. Because optional components such as PowerShell or other script engines might not be supported for installation on all VCM-supported OS versions, a `Not Executed` status does not result in a failure.
- Collect Windows Custom Information. See "Collect Windows Custom Information Data" on page 106.

Procedure

1. On your VCM Collector, click **Administration**.
2. Select **Job Manager > History > Instant Collections > Past 24 Hours**.
3. In the Instant Collections pane, select a collection job that includes WCI data.
4. In the Job History Machine Detail pane, select **View Details**.

   A single row appears for each WCI filter that ran in the collection job. Information about the WCI script and the script results parsing appears in the row.
5. In the View Details by Machine window, select the managed machines to view and click **OK**.

   Detailed job history results appear for the WCI filters and managed machines.

   - If a WCI collection job encounters errors on a VCM managed machine, VCM reports detailed information about the failure. Failures can occur when PowerShell starts, during script execution, or when interpreting the script results.
   - If PowerShell is not installed on the managed machine, an error can occur in the PowerShell startup process. Because PowerShell is an optional component, a status of `Not Executed` can appear in the job details to indicate the skipped steps. The `Not Executed`status does not appear as an error in the VCM job.
   - If a PowerShell script generates errors due to defects in the script, such as syntactical or typographical errors, VCM reports the status as finished with errors in the collection job.

What to do next

- Review the WCI collection results. See "Windows Custom Information Collection Results" on page 109.
- Generate your own reports. See "Run Windows Custom Information Reports" on page 110.

Windows Custom Information Collection Results

Examine the results of your Windows Custom Information (WCI) collected data in the VCM tree views and list view.

Prerequisites

Collect WCI data and confirm that the WCI collection job finished. Click **Administration** and select **Job Manager > History > Other Jobs > Past 24 Hours**. See "Collect Windows Custom Information Data" on page 106.

Procedure

1. On your VCM Collector, click **Console**.
2. Select **Windows > Operating System > Custom Information**.
3. Select a view of the collected WCI data.

Option	Description
Tree View - Standard	Tree hierarchy view based on the data structure in your PowerShell script.
Tree View - Consolidated	Tree hierarchy that displays data across multiple elements simultaneously with the data consolidated from one level of the tree. The child node properties and values appear in each node.
List View	Data organized by a list of top-level elements. You can filter, sort, or group the data.

What to do next

Generate your own reports. See "Run Windows Custom Information Reports" on page 110.

Run Windows Custom Information Reports

Generate your own reports or run existing reports on Windows Custom Information (WCI) data that you collected using your custom PowerShell scripts.

Prerequisites

Collect WCI data. See "Collect Windows Custom Information Data" on page 106.

Procedure

1. On your VCM Collector, click **Reports**.
2. Select **Machine Group Reports > Windows > Custom Information**.
3. Select a custom information report.

Option	Description
Netstat Open Ports Information	Reports port and protocol information from the `netstat -A` command.
SQL SMO Database Information	Reports the database details collected.
SQL SMO Instance Information	Reports basic information about the SQL Server instances collected.

4. Click **Run**.

   The report displays detailed information about the collected WCI data. For example, the NetStat Open Ports Information report displays the protocol, port, remote port, local address, foreign address, port state, and the collection filter used in the collection.

Troubleshooting Custom PowerShell Scripts

If you encounter problems when you run custom PowerShell scripts, run the script as a `.ps1` file and correct any errors before you use the script with a VCM collection filter.

Prerequisites

- Verify that your script runs in PowerShell. See "Verify that Your Custom PowerShell Script is Valid" on page 105.
- Understand the PowerShell script signing policies. See "PowerShell Script Signing Policies" on page 97.

Procedure

1. On your VCM Collector, save the script to a file that has the `.ps1` extension.
2. Run the script file from a command line using PowerShell 2.0 or PowerShell 1.0.
   - For PowerShell 2.0, run:
     ```
     PowerShell –command set-executionpolicy RemoteSigned –scope Process ;
     scriptname.ps1 > resultfile.xml
     ```
   - For PowerShell 1.0, set the execution policy to Remote Signed or use a less restrictive policy, and run:
     ```
     PowerShell –file scriptname.ps1 > resultfile.xml
     ```

   When the script is finished running, it generates the XML file.
3. Verify that you can open the XML file in Internet Explorer.
   - If you cannot see the entire file, allow blocked content.
   - If Internet Explorer cannot parse the XML file, you must correct any formatting errors.

   If you have Visual Studio installed, you can use it locate formatting errors in large XML files.

What to do next

- Re-run your custom PowerShell script. See "Collect Windows Custom Information Data" on page 106.
- To confirm that the job finished running, click **Administration** and select **Job Manager > History > Other Jobs > Past 24 Hours**.
- View the detailed status about exit codes and standard error output for each job that processed the script or filter. See "View Windows Custom Information Job Status Details" on page 108.
- After the Windows Custom Information data is available in the VCM database, you can generate reports and enforce compliance. See the online help.

Discover, License, and Install UNIX/Linux Machines

To collect UNIX/Linux data and to manage your physical or virtual UNIX/Linux machines, you must add the machines, license them for use, and install the appropriate VCM Agent.

Prerequisites

Review the upgrade requirements to determine if the machines on which you are installing the current Agent are supported platforms and machine type. See "Upgrade Requirements for UNIX/Linux Machines" on page 112.

Procedure

1. "Add UNIX/Linux Machines" on page 112

   Add UNIX/Linux machines to the Available UNIX Machines list to make the machines available for licensing.

2. "License UNIX/Linux Machines" on page 114

   License UNIX/Linux machines before you install the Agent and begin to manage them. You license the machines displayed in the Available UNIX Machines list.

3. "Install the Agent on UNIX/Linux Machines" on page 114

   Install the appropriate version of the VCM Agent on each of your licensed target machines to enable communication between the Collector and the managed UNIX/Linux machines.

4. "Collect UNIX/Linux Data" on page 121

   When the UNIX/Linux machines are licensed and the Agent is installed, you collect data from those machines.

Continuous machine management is based on the latest data you collect from target machines. You can view data and run actions, such as reports or compliance, based on the collected data. See "UNIX/Linux Collection Results" on page 121.

Upgrade Requirements for UNIX/Linux Machines

To use new VCM functionality, you must upgrade the Agent on target machines based on machine type. You must consider several requirements if you are upgrading from a previous Agent version to the current version on your managed UNIX/Linux machines.

General UNIX/Linux machine requirements are specified in the *VCM Hardware and Software Requirements Guide*.

Upgrading Red Hat Workstations

When you upgrade the UNIX Agent on Red Hat machines, be aware of the licensing changes between versions of VCM. Prior to VCM 5.2, Red Hat workstations and servers were licensed as Red Hat servers. In VCM 5.2, Red Hat machines were licensed as either workstations or servers.

When you upgrade to VCM 5.2 or later, Red Hat workstations that were previously managed with server licenses are not managed in VCM. Unmanaged Red Hat machines appear in the Available UNIX Machines list before you license them. To license these machines, click **Administration**, select **Machines Manager > Available Machines > Available UNIX Machines**, and re-license the machines using the Linux/Mac Workstation licenses.

For help to identify your unmanaged Red Hat machines, contact VMware Technical Support.

Add UNIX/Linux Machines

Add UNIX/Linux machines to the Available UNIX Machines list to make the machines available for licensing.

If you add a large number of machines, you can use other methods to add the machines. See the online help for procedures to import machine information from a file or use IP Discovery.

NOTE The Discovered Machines Import Tool (DMIT) can import many physical and virtual machines at one time into the VCM database. The tool imports machines discovered by the Network Mapper (Nmap). Download DMIT from the VMware Web site.

Prerequisites

Verify that you know the name or IP address, domain, domain type, machine type, and the communication port for the machines to add.

Procedure

1. Click **Administration**.
2. Select **Machines Manager > Available Machines > Available UNIX Machines**.
3. Click **Add Machines**.
4. On the Add Machines page, select **Basic** and click **Next**.
5. On the Manually Add Machines - Basic page, add the machine information.
   a. Configure machine information.

Option	Action
Machine	Type the name of the machine. You can use NetBIOS or Fully-Qualified Domain Name (FQDN) notation for the name. If your Collector cannot resolve a host name with a DNS Server, use an IP address rather than a machine name.
Domain	Type or select the domain to which the machine belongs.
Type	Select the domain type.
Machine Type	Select the machine type.
Port	Type the port number. The default value is 26542. This option appears only when you select a UNIX/Linux or Mac OS X machine type. The port number must be the same number used when you install the Agent on the managed UNIX/Linux machine.

   b. Click **Add**.

      The machine is added to the list.

   c. To add other machines, configure the machine information and click **Add**.

   d. After you add the target machines, click **Next**.

6. On the Important page, review the machine information and click **Finish**.

   The machine is added to the Available UNIX Machines data grid.

What to do next

License the machine. See "License UNIX/Linux Machines" on page 114.

License UNIX/Linux Machines

License UNIX/Linux machines before you install the Agent and begin to manage them. You license the machines displayed in the Available UNIX Machines list.

Prerequisites

- Verify that you added the machines. See "Add UNIX/Linux Machines" on page 112.
- Determine if your managed Red Hat workstations and servers are affected by an upgrade from a previous version of VCM. See "Upgrade Requirements for UNIX/Linux Machines" on page 112.
- Verify that the machines you are licensing have a specified Machine Type. Machines without a Machine Type value will not be licensed.

Procedure

1. Click **Administration**.
2. Select **Machines Manager > Available Machines > Available UNIX Machines**.
3. Select the machines and click **License**.
4. On the Machines page, verify that the Selected list includes the machines to license and click **Next**.
5. On the Product License Details page, review the licensed machine count and click **Next**.
6. On the Important page, click **Finish**.

What to do next

Install the Agent on the target machines. See "Install the Agent on UNIX/Linux Machines" on page 114.

Install the Agent on UNIX/Linux Machines

Install the appropriate version of the VCM Agent on each of your licensed target machines to enable communication between the Collector and the managed UNIX/Linux machines.

Installing the Agent on UNIX/Linux machines is a manual operation. You can run the installation process in silent mode or interactive mode. To run the installation in silent mode, you must edit the configuration options in the `csi.config` file. The file is edited to accommodate different target machine types.

A Deployment Utility is available in `C:\Program Files (x86)\VMware\VCM\Tools` to assist you with your UNIX/Linux configuration for selected steps. See the utility's online help for more information.

IMPORTANT Ensure you install the Agent on newly managed machines rather than upgrading currently managed machines. If you are upgrading, see the online help and "Upgrade Requirements for UNIX/Linux Machines" on page 112.

Prerequisites

- Verify that the machine on which you intend to install the Agent has enough free disk space. For more information, see the *VCM Hardware and Software Requirements Guide*.
- If you run an installation in silent mode, modify the appropriate `csi.config` file variable options. See "Installation Options for UNIX/Linux csi.config " on page 118.
- If you select `(x)inetd/launchd` for `CSI_AGENT_RUN_OPTION`, verify that `(x)inetd/launchd` is running on the target machines. On some versions, when `(x)inetd/launchd` services are not configured, `(x)inetd/launchd` will not stay running. To ensure the Agent installation completes successfully, pass a `- stayalive` option to `(x)inetd/launchd`. See "Installation Options for UNIX/Linux csi.config " on page 118.
- Log on to the target UNIX/Linux machine as `root`.
- Disable or reconfigure firewalls on SUSE and Red Hat machines to install the Agent.
- Select the method you want to use to copy files to the target machines. You can use `ftp`, `sftp`, or `cp` using an NFS share. If you use `ftp` to copy the package to your machine, you must use binary mode.

Procedure

1. Copy the appropriate Agent binary installation package from the Collector to the machine on which you will install the Agent.

   The Agent packages are located on the Collector in `\Program Files (x86)\VMware\VCM\Installer\Packages`.

Operating System Version	Agent Binary
Red Hat (Enterprise) Linux Edition (Version 3.0, 4.0, 5.0, 5.1, 5.2, 5.3, 5.4, 5.5, 6) SUSE Linux Enterprise Server (9, 10, 11, 11.1), Debian (4)	`CMAgent.<version>.Linux`
Solaris (Versions 9 and 10 supported on Sparc)	`CMAgent.<version>.SunOS`
Solaris (Version 10 for x86)	`CMAgent.<version>.SunOS.x86.5.10`
HP-UX 11i Versions 1.0, 2.0, 3.0 (11.11, 11.23, and 11.31; Supported on PA-RISC)	`CMAgent.<version>.HP-UX.11.pa`
HP-UX 11i Version 2.0, 3.0 (11.23 and 11.31-Supported on Itanium)	`CMAgent.<version>.HPUX.11.ia64`
AIX Version 5L (5.3 and 6L (6.1))	`CMAgent.<version>.AIX.5`

2. On the target machine, run `chmod u+x <filename>` to set the execute permission for the file owner on the Agent binary file.
3. In the directory to which you copied the file, run `./CMAgent.<version>.<Agent binary name>` to create the necessary directory structure and extract the files.

   To force an overwrite of any existing files, include the `-o` option. For example: `/CMAgent.<version>.SunOS -o`.

   The command and output is similar to the following example, but with different file names depending on the operating system.

```
# ./CMAgent.<version>.SunOS
UnZipSFX 5.51 of 22 May 2004, by Info-ZIP (http://www.info-zip.org).
creating: CSIInstall/
creating: CSIInstall/packages/
inflating: CSIInstall/packages/Agent.1.0.SunOS
inflating: CSIInstall/packages/CFC.1.0.SunOS
inflating: CSIInstall/packages/ECMu.1.0.SunOS
inflating: CSIInstall/packages/ThirdParty.1.0.SunOS
inflating: CSIInstall/packages/cis.1.0.SunOS
extracting: CSIInstall/packages/package.sizes.SunOS
inflating: CSIInstall/packages/python.23.SunOS
creating: CSIInstall/scripts/
inflating: CSIInstall/scripts/checksum
inflating: CSIInstall/scripts/BootStrapInstall.sh
inflating: CSIInstall/scripts/AltSource_filesystem.sh
inflating: CSIInstall/scripts/AltSource_ftp.sh
inflating: CSIInstall/scripts/AltSource_rcp.sh
inflating: CSIInstall/scripts/AltSource_sftp.sh
inflating: CSIInstall/scripts/AltSource_wget.sh
extracting: CSIInstall/scripts/AltSourceCmd
inflating: CSIInstall/InstallCMAgent
inflating: CSIInstall/csi.config
inflating: CSIInstall/CMAgent.<version.OS>
creating: CSIInstall/.security/certificates/
inflating:CSIInstall/.security/certificates/<EnterpriseCertificate>
```

4. Run `cd <extractedpath>/CSIInstall` to change the directory to the location where the `InstallCMAgent` executable file was extracted.
5. Run `ls -la` to validate that the correct files are in the `<extractedpath>/CSIInstall` directory.

File	Description
`InstallCMAgent`	Installation script.
`csi.config`	Configuration file for the installation. This is the file you can modify to include installation options for silent rather than interactive installation processes.
`packages`	Installation packages.
`scripts`	Scripts required for the installation.

6. (Optional) Edit the `csi.config` file to customize the installation variables and save your changes.
   a. Run the `chmod u+x csi.config` command to add write file permissions if the file has only read permissions set.
   b. Modify the `csi.config` file options based on your local requirements and save the file.
   c. Copy the modified and saved `csi.config` file to the extracted location.

      For example, `# cp /<safelocation>/csi.config /<extractedlocation>/CSIInstall/csi.config`.
7. Run `InstallCMAgent` in either silent mode or interactive mode.

Option	Action
Silent mode	Run the `# ./CSIInstall/InstallCMAgent -s` command. Install the Agent using the silent mode if you manually edited the `csi.config` file, if you modified the `csi.config` file using the interactive method, or if you are using a custom configuration file that you saved from a previous Agent installation. This mode uses the values specified in `csi.config` without prompting for input. When the silent installation completes, a summary of the installation process and status appears. Verify that the installation completed without errors.
Interactive mode	Run the `# ./CSIInstall/InstallCMAgent` command. Install the Agent using the interactive mode if you did not modify the `csi.config` and if you want to respond to each prompt to accept or change each parameter in the `csi.config` file as it runs. As a result of your responses, the `csi.config` is modified. The pre-installation stage of interactive mode checks for a valid user, `CSI_USER`. If the user exists, you are not prompted for these configuration values. ■ `CSI_USER_NO_LOGIN_SHELL` ■ `CSI_USER_PRIMARY_GROUP` ■ `CSI_USER_PRIMARY_GID` ■ `CSI_USER_USE_NEXT_AVAILABLE_LOCAL_GID` You are prompted for these values only when the `CSI_USER` user account is not found.

You can check the installation status in the installation log file. The file is located in `<CSI_PARENT_DIRECTORY>/log/install.log`.

8. Run `ls -la /CSI_PARENT_DIRECTORY/CMAgent` to verify that all the required files and directories were installed.

   `/CSI_PARENT_DIRECTORY/CMAgent` is the default directory. If you changed the directory name during installation, modify the `ls -la` command to display the custom directory name.

```
drwxr-x--- 3 root cfgsoft 4096 Jul 2 17:34 Agent
drwxr-x--- 3 root cfgsoft 4096 Jul 2 17:34 CFC
-rw-rw---- 1 root cfgsoft 49993 Jul 2 17:34 CSIRegistry
-rw-rw---- 1 root cfgsoft 0 Jul 2 17:34 .CSIRegistry.lck
drwxrwx--- 3 csi_acct cfgsoft 4096 Jul 2 17:34 data
```

```
drwxrwx--- 3 root cfgsoft 4096 Jul 2 17:34 ECMu
drwxr-x--- 6 root cfgsoft 4096 Jul 2 17:34 install
lrwxrwxrwx 1 root root 20 Jul 2 17:34 log -> /var/log/CMAgent/log
dr-xr-x--x 3 root cfgsoft 4096 Jul 2 17:34 ThirdParty
drwxr-xr-x 2 root root 4096 Jul 2 17:34 uninstall
```

9. Run `# netstat -na | grep <port_number>` to verify that the Agent is installed correctly, listening on the assigned port, and ready to collect data.

   The default <port_number> is 26542 for VCM installations.

10. If you are installing on SUSE, you should start `xinetd` using the `# ./etc/init.d/xinetd start` command after the installation completes.

What to do next

Run a collection for UNIX/Linux data. See "Collect UNIX/Linux Data" on page 121

Installation Options for UNIX/Linux csi.config

The installation options are variables you add or modify in the `csi.config` file used when you install the Agent. You can create several versions of this file based on operating system or specific settings, but you must not change the file name.

Installation Options with Default Values	Description
`CSI_AGENT_RUN_OPTION`	You can install the Agent as a daemon process or installed to be run by `inetd/xinetd/launchd`. ■ A value of inetd installs the Agent for execution by `inetd/xinetd/launchd`. ■ A value of daemon installs the agent for execution as a daemon process.

`CSI_NO_LOGIN_SHELL=`
`+S:+A`
`:+/sbin/noshell+/bin/false+`
`/sbin/false+/usr/bin/false`
`+/sbin/nologin`
	The `CSI_USER` account must not have a login shell. This parameter lists all valid no-login shells and is used to verify the `CSI_USER` has no-login shell.
	If your system has a valid no login shell that is not listed, you append a plus sign and add the no login shell to the list.
	The options available for this parameter include:
	■ `+S` means only for Solaris
	■ `+A` means only for AIX
	■ `+H` means only for HP-UX
	■ `+L` means only for Linux
	■ `+` means for all operating systems

`CSI_CREATE_USER=Y` Keep the default value	Indicates whether or not the user will be created. When you install in trusted mode on HP-UX v1.0 (11.11), the user must already exist on the target machine. If you attempt to install and create the user, the installation of the Agent fails.
`CSI_USER_ID=501` Keep the default value	Integer value for the user ID of the created user.

Installation Options with Default Values	Description
CSI_USER_NO_LOGIN_SHELL=/bin/false Keep the default value	Indicates the desired no-login shell value to use when you create the user.
CSI_USER_PRIMARY_GROUP=csi_acct Keep the default value	Group name to use when you create a new user as the user's primary group. This group is for low security access. Most inspections are executed with the lowest possible privileges using this group while also preventing access by way of this group to the high security group privileges.
CSI_CREATE_USER_PRIMARY_GROUP=Y Keep the default value	Indicates the need to create a low-security primary group for the CSI_USER.
CSI_USER_PRIMARY_GID=501Keep the default value	Create user's primary Group ID.
CSI_USER_USE_NEXT_AVAILABLE_LOCAL_GID=Y Keep the default value	Setting this option to Y allows the Group ID to be the next available local Group ID over CSI_USER_PRIMARY_GID.
CSI_USER=csi_acct Keep the default value	The user assigned to the cfgsoft group. The CSI listener process runs under this user.
CSI_CFGSOFT_GID=500 Keep the default value	The Group ID of the cfgsoft group. This value can change if the GID is already in use. This group is for high-security access. Some inspections require root privileges, which are provided indirectly through this group and setuid to root.
CSI_CREATE_LOCAL_GROUP=Y Keep the default value	Setting this option to Y allows the cfgsoftgroup to be created. This setting allows the system call to groupadd.
CSI_USE_NEXT_AVAILABLE_LOCAL_GID=Y Keep the default value	Setting this option to Y allows this Group ID to be the next available local Group ID starting at CSI_CFGSOFT_GID.
CSI_AGENT_PORT=26542 Keep the default value	Specifies the port on which the Agent listens.
CSI_CREATE_LOCAL_SERVICE=YKeep the default value	Setting CSI_CREATE_LOCAL_SERVICE to Yallows the system to create the local service (copy files to system directories).
CSI_REFRESH_INETD=Y Keep default value only if you are running your agent as inetd. If you are running your agent as a daemon, select CSI_REFRESH_INETD=N	Setting this option to Y allows the system to refresh xinetd (Linux) or inetd (Solaris, AIX, and HP-UX).
CSI_NICE=10 Keep the default value	Sets the nice value for the agent listener process.

Installation Options with Default Values	Description
CSI_CERTIFICATE_PATH=	Specifies the path to Collector Certificates. The certificates specified at this path are copied to the Agent. If your Collector Certificates are stored in an accessible location on this machine, you use this option to put the certificates in the Agent location. You should install the Enterprise Certificates so that multiple collector instances collecting from the same set of Agents is supported. If this package was copied from a collector installation, this package already contains that Collector's Enterprise Certificate.
CSI_PARENT_DIRECTORY=/opt	Specifies the parent directory of the CM Agent. The root directory of CMAgent will be CSI_PARENT_DIRECTORY/CMAgent.
CSI_PARENT_DATA_ DIRECTORY=/opt	Specifies the parent directory of the CMAgent data directory. The data directory will be CSI_PARENT_DATA_DIRECTORY/ CMAgent/data.
CSI_PARENT_LOG_ DIRECTORY=default	Specifies where agent operational log files are kept. The log directory is CSI_PARENT_LOG_DIRECTORY/CMAgent/log. The default value indicates to use these values. ■ Linux: /var/log ■ AIX, HP-UX, and Solaris: /var/adm
CSI_KEEP_CSIINSTALL=N Recommend keeping default value.	After a successful installation, the temp installation directory CSIInstall is deleted. To keep this installation directory, set this parameter to Y.

Manually Uninstall the UNIX/Linux Agent

When you install the Agent, an uninstall file, UninstallCMAgent, is automatically created in <path>/CMAgent/uninstall. You use the file to manually uninstall the Agent from the managed machine.

The uninstall reverses all changes made by installation. However, the installation log files are retained in <AgentRoot>/install. <AgentRoot> defaults to the CMAgent directory that was created during installation.

Prerequisite

Determine if you want to save a copy of the configuration file for use on other machines. If you do, copy csi.config, the file that contains all of the custom configuration settings, to a secure location. The file is located in <path>/CMAgent/install.

Procedure

1. Navigate up one level from the uninstall directory in the CMAgent directory.
2. Run the # ./uninstall/UninstallCMAgent command to uninstall the Agent.

What to do next

After you run UninstallCMAgent, delete the remaining the CMAgent directory before you install a new Agent.

Collect UNIX/Linux Data

When the UNIX/Linux machines are licensed and the Agent is installed, you collect data from those machines.

Collecting data from machines adds the collected machine information to the VCM database and makes the machine data available for reporting, running compliance, and other management options. The collection process for UNIX/Linux collection is similar to other collections, including Windows, except that you select UNIX data types during the collection instead of Windows data types.

Prerequisites

- License the target machines. See "License UNIX/Linux Machines" on page 114.
- Install the Agent on the target machines. See "Install the Agent on UNIX/Linux Machines" on page 114.

Procedure

1. On the toolbar, click **Collect**.
2. On the Collection Type page, select **Machine Data** and click **OK**.
3. On the Machines page, select the machines from which you are collecting data and click **Next**.
4. On the Data Types page, configure the collection and click **Next**.
   a. Select the **Select All** check box.
   b. Select **Use default filters**.
5. On the Important page, verify that there are no conflicts with previously scheduled or running jobs, and click **Finish**.

   The amount of time the first collection requires is determined by the number of machines and network connectivity.
6. Click Administration and select **Job Manager > History > Instant Collections > Past 24 Hours** to determine if the collection finished.

What to do next

- Review your collected data. See "UNIX/Linux Collection Results" on page 121.

Updates to UNIX Patch Assessment Content Affects UNIX Agent Performance

By default, VCM Patching checks for patch updates every 4 hours. The time required to perform this action depends on the amount of new content downloaded to the Collector during the update process.

When the UNIX patch assessment content is pushed out to the UNIX Agents, the time required to run jobs such as collections and remote commands increases slightly. The time required varies based on how much new or updated content must be synchronized between the Collector and the Agent. This content push occurs when the first communication is initiated after installing the UNIX Agent package, or when the Collector has platform-applicable patch content that was added after the last communication between the Agent and the Collector.

UNIX/Linux Collection Results

UNIX/Linux data is displayed in VCM and is available for several management actions.

The displayed data is only as current as the last time you collected the data.

Option	Description
Console	Displays dashboards and reports based on collected data. You use the Console to view data relevant to day-to-day operations, troubleshooting, and analysis. To view the dashboards, click **Console** and select **Dashboards > UNIX**. To view the summary reports, click **Console** and select **UNIX tab > Operating System > Machines > General**. You can view the data in a summary report or data grid format.
Reports	Runs pre-configured VCM reports or create custom reports. Reports are run against currently collected data. Depending on the volume or complexity of the data requested in a report, it may take time to generate the report. Refer to the online help for information about scheduling and disseminating reports. To use the reporting options, click **Reports** and select **Machine Group Reports > UNIX**.
Compliance	Determines if the collected data from target machines meets specified compliance values, and allows you to run compliance remediation actions. To run a compliance check, click **Compliance** and select **Machine Group Compliance** and follow the steps described in the online help to create rule groups, rules, filters, and templates.
Patching	Assesses target machines to determine if the machines have the most current patches. If the patches are not yet installed, you can install the latest patches on the target machines. To assess and patch machines, select **Patching**, and then select your target operating system.

Discover, License, and Install Mac OS X Machines

To collect Mac OS X data and to manage your physical or virtual Mac OS X machines, you must add the machines, license them for use, and install the appropriate VCM Agent.

Mac OS X machines are managed in conjunction with UNIX machines.

Procedure

1. "Add Mac OS X Machines" on page 123

   Add Mac OS X machines to the Available UNIX Machines list to make the machines available for licensing.

2. "License Mac OS X Machines" on page 124

   License Mac OS X machines before you install the Agent and begin to manage them. You license the machines displayed in the Available UNIX Machines list.

3. "Install the Agent on Mac OS X Machines" on page 124

   Install the appropriate version of the VCM Agent on each of your licensed target machines to enable communication between the Collector and the managed Mac OS X machines.

4. "Collect Mac OS X Data" on page 129

   When the Mac OS X machines are licensed and the Agent is installed, you collect data from those machines.

Continuous machine management is based on the latest data you collect from target machines. You can view data and run actions, such as reports or compliance, based on the collected data. See "UNIX/Linux Collection Results" on page 121.

Add Mac OS X Machines

Add Mac OS X machines to the Available UNIX Machines list to make the machines available for licensing.

If you add a large number of machines, you can use other methods to add the machines. See the online help for procedures to import machine information from a file or use IP Discovery.

NOTE The Discovered Machines Import Tool (DMIT) can import many physical and virtual machines at one time into the VCM database. The tool imports machines discovered by the Network Mapper (Nmap). Download DMIT from the VMware Web site.

Prerequisites

Verify that you know the name or IP address, domain, domain type, machine type, and the communication port for the machines to add.

Procedure

1. Click **Administration**.
2. Select **Machines Manager > Available Machines > Available UNIX Machines**.
3. Click **Add Machines**.
4. On the Add Machines page, select **Basic** and click **Next**.
5. On the Manually Add Machines - Basic page, add the machine information.
   a. Configure machine information.

Option	Action
Machine	Type the name of the machine. You can use NetBIOS or Fully-Qualified Domain Name (FQDN) notation for the name. If your Collector cannot resolve a host name with a DNS Server, use an IP address rather than a machine name.
Domain	Type or select the domain to which the machine belongs.
Type	Select the domain type.
Machine Type	Select the machine type.
Port	Type the port number. The default value is 26542. This option appears only when you select a UNIX/Linux or Mac OS X machine type. The port number must be the same number used when you install the Agent on the managed Mac OS X machine.

   b. Click **Add**.

      The machine is added to the list.

   c. To add other machines, configure the machine information and click **Add**.

   d. After you add the target machines, click **Next**.

6. On the Important page, review the machine information and click **Finish**.

   The machine is added to the Available UNIX Machines data grid.

What to do next

License the machine. See "License Mac OS X Machines" on page 124.

License Mac OS X Machines

License Mac OS X machines before you install the Agent and begin to manage them. You license the machines displayed in the Available UNIX Machines list.

Prerequisites

- Verify that you added the machines. See "Add Mac OS X Machines" on page 123.
- Verify that the machines you are licensing have a specified Machine Type. Machines without a Machine Type value will not be licensed.

Procedure

1. Click **Administration**.
2. Select **Machines Manager > Available Machines > Available UNIX Machines**.
3. Select the machines and click **License**.
4. On the Machines page, verify that the Selected list includes the machines to license and click **Next**.
5. On the Product License Details page, review the licensed machine count and click **Next**.
6. On the Important page, click **Finish**.

What to do next

Install the Agent on the target machines. See "Install the Agent on Mac OS X Machines" on page 124

Install the Agent on Mac OS X Machines

Install the appropriate version of the VCM Agent on each of your licensed target machines to enable communication between the Collector and the managed Mac OS X machines.

Installing the Agent on Mac OS X machines is a manual operation. The Agent is packaged as a Universal Binary Installer. You can run the installation process in silent mode or interactive mode. To run the installation in silent mode, you must edit the configuration options in the `csi.config` file. The file is edited to accommodate different target machine types.

Prerequisites

- Verify that the machine on which you intend to install the Agent has enough free disk space. For more information, see the *VCM Hardware and Software Requirements Guide*.
- If you run an installation in silent mode, modify the appropriate `csi.config` file variable options. See "Installation Options for Max OS X csi.config " on page 127.
- If you select `(x)inetd/launchd` for `CSI_AGENT_RUN_OPTION`, verify that `(x)inetd/launchd` is running on the target machines. On some versions, when `(x)inetd/launchd` services are not configured, `(x)inetd/launchd` will not stay running. To ensure the Agent installation completes successfully, pass a `- stayalive` option to `(x)inetd/launchd`. See "Installation Options for Max OS

- Log on to the target Mac OS X machine as `root`, or have `sudo` as `root`.
- Select the method you want to use to copy files to the target machines. You can use `ftp`, `sftp`, or `cp` using an NFS share. If you use `ftp` to copy the package to your machine, you must use binary mode.

Procedure

1. Copy the appropriate Agent binary installation package from the Collector to the machine on which you will install the Agent.

   The Agent packages are located on the Collector in `\Program Files (x86)\VMware\VCM\Installer\Packages`.

Operating System Version	Agent Binary
Mac OS X (Version 10.5 and 10.6)	`CMAgent.<version>.Darwin`

2. On the target machine, run `chmod u+x <filename>` to set the execute permission for the file owner on the Agent binary file.
3. In the directory to which you copied the file, run `./CMAgent.<version>.<Agent binary name>` to create the necessary directory structure and extract the files.

   To force an overwrite of any existing files, include the `-o` option. For example: `/CMAgent.<version>.Darwin -o`.

   The command and output is similar to the following example, but with different file names depending on the operating system.

```
# ./CMAgent.<version>.Darwin
UnZipSFX 5.51 of 22 May 2004, by Info-ZIP (http://www.info-zip.org).
creating: CSIInstall/
inflating: CSIInstall/CMAgent.5.1.0.Darwin.i386
inflating: CSIInstall/CMAgent.5.1.0.Darwin.ppc
inflating: CSIInstall/csi.config
inflating: CSIInstall/InstallCMAgent
```

4. Run `cd <extractedpath>/CSIInstall` to change the directory to the location where the `InstallCMAgent` executable file was extracted.
5. Run `ls -la` to validate that the correct files are in the `<extractedpath>/CSIInstall` directory.

File	Description
`InstallCMAgent`	Installation script.
`csi.config`	Configuration file for the installation. This is the file you can modify to include installation options for silent rather than interactive installation processes.
`packages`	Installation packages.
`scripts`	Scripts required for the installation.

6. (Optional) Edit the `csi.config` file to customize the installation variables and save your changes.

a. Run the `chmod u+x csi.config` command to add write file permissions if the file has only read permissions set.

b. Modify the `csi.config` file options based on your local requirements and save the file.

c. Copy the modified and saved `csi.config` file to the extracted location.

   For example, `# cp /<safelocation>/csi.config /<extractedlocation>/CSIInstall/csi.config`.

7. Run `InstallCMAgent` in either silent mode or interactive mode.

Option	Action
Silent mode	Run the `# ./CSIInstall/InstallCMAgent -s` command. Install the Agent using the silent mode if you manually edited the `csi.config` file, if you modified the `csi.config` file using the interactive method, or if you are using a custom configuration file that you saved from a previous Agent installation. This mode uses the values specified in `csi.config` without prompting for input. When the silent installation completes, a summary of the installation process and status appears. Verify that the installation completed without errors.
Interactive mode	Run the `# ./CSIInstall/InstallCMAgent` command. Install the Agent using the interactive mode if you did not modify the `csi.config` and if you want to respond to each prompt to accept or change each parameter in the `csi.config` file as it runs. As a result of your responses, the `csi.config` is modified. The pre-installation stage of interactive mode checks for a valid user, `CSI_USER`. If the user exists, you are not prompted for these configuration values. ■ `CSI_USER_NO_LOGIN_SHELL` ■ `CSI_USER_PRIMARY_GROUP` ■ `CSI_USER_PRIMARY_GID` ■ `CSI_USER_USE_NEXT_AVAILABLE_LOCAL_GID` You are prompted for these values only when the `CSI_USER` user account is not found. The User and the Group are created in the local directory service storage.

You can check the installation status in the installation log file. The file is located in `<CSI_PARENT_DIRECTORY>/log/install.log`.

8. Run `ls -la /CSI_PARENT_DIRECTORY/CMAgent` to verify that all the required files and directories

were installed.

`/CSI_PARENT_DIRECTORY/CMAgent` is the default directory. If you changed the directory name during installation, modify the `ls -la` command to display the custom directory name.

```
drwxr-x--- 3 root cfgsoft 4096 Jul 2 17:34 Agent
drwxr-x--- 3 root cfgsoft 4096 Jul 2 17:34 CFC
-rw-rw---- 1 root cfgsoft 49993 Jul 2 17:34 CSIRegistry
-rw-rw---- 1 root cfgsoft 0 Jul 2 17:34 .CSIRegistry.lck
drwxrwx--- 3 csi_acct cfgsoft 4096 Jul 2 17:34 data
drwxrwx--- 3 root cfgsoft 4096 Jul 2 17:34 ECMu
drwxr-x--- 6 root cfgsoft 4096 Jul 2 17:34 install
lrwxrwxrwx 1 root root 20 Jul 2 17:34 log -> /var/log/CMAgent/log
dr-xr-x--x 3 root cfgsoft 4096 Jul 2 17:34 ThirdParty
drwxr-xr-x 2 root root 4096 Jul 2 17:34 uninstall
```

9. Run `# netstat -na | grep <port_number>` to verify that the Agent is installed correctly, listening on the assigned port, and ready to collect data.

   The default <port_number> is 26542 for VCM installations.

What to do next

Run a collection for Mac OS X data. See "Collect Mac OS X Data" on page 129.

Installation Options for Max OS X csi.config

The installation options are variables you add or modify in the `csi.config` file used when you install the Agent. You can create several versions of this file based on operating system or specific settings, but you must not change the file name.

Installation Options with Default Values	Description
`CSI_AGENT_RUN_OPTION`	You can install the Agent as a daemon process or installed to be run by `inetd/xinetd/launchd`. ■ A value of inetd installs the Agent for execution by `inetd/xinetd/launchd`. ■ A value of daemon installs the agent for execution as a daemon process.

`CSI_NO_LOGIN_SHELL=`
`+D`
`:+/sbin/noshell+/bin/false+`
`/sbin/false+/usr/bin/false`
`+/sbin/nologin`
	The `CSI_USER` account must not have a login shell. This parameter lists all valid no-login shells and is used to verify the `CSI_USER` has no-login shell.
	If your system has a valid no login shell that is not listed, you append a plus sign and add the no login shell to the list.
	The options available for this parameter include:
	■ `+D` means only for Darwin (Mac OS X)
	■ `+` means for all operating systems

`CSI_CREATE_USER=Y` Keep the default value	Indicates whether or not the user will be created.
`CSI_USER_ID=501` Keep the default value	Integer value for the user ID of the created user.

Installation Options with Default Values	Description
CSI_USER_NO_LOGIN_SHELL=/bin/false Keep the default value	Indicates the desired no-login shell value to use when you create the user.
CSI_USER_PRIMARY_GROUP=csi_acct Keep the default value	Group name to use when you create a new user as the user's primary group. This group is for low security access. Most inspections are executed with the lowest possible privileges using this group while also preventing access by way of this group to the high security group privileges.
CSI_CREATE_USER_PRIMARY_GROUP=Y Keep the default value	Indicates the need to create a low-security primary group for the CSI_USER.
CSI_USER_PRIMARY_GID=501Keep the default value	Create user's primary Group ID.
CSI_USER_USE_NEXT_AVAILABLE_LOCAL_GID=Y Keep the default value	Setting this option to Y allows the Group ID to be the next available local Group ID over CSI_USER_PRIMARY_GID.
CSI_USER=csi_acct Keep the default value	The user assigned to the cfgsoft group. The CSI listener process runs under this user.
CSI_CFGSOFT_GID=500 Keep the default value	The Group ID of the cfgsoft group. This value can change if the GID is already in use. This group is for high-security access. Some inspections require root privileges, which are provided indirectly through this group and setuid to root.
CSI_CREATE_LOCAL_GROUP=Y Keep the default value	Setting this option to Y allows the cfgsoftgroup to be created. This setting allows the system call to groupadd.
CSI_USE_NEXT_AVAILABLE_LOCAL_GID=Y Keep the default value	Setting this option to Y allows this Group ID to be the next available local Group ID starting at CSI_CFGSOFT_GID.
CSI_AGENT_PORT=26542 Keep the default value	Specifies the port on which the Agent listens.
CSI_CREATE_LOCAL_SERVICE=YKeep the default value	Setting CSI_CREATE_LOCAL_SERVICE to Yallows the system to create the local service (copy files to system directories).
CSI_REFRESH_INETD=Y Keep default value only if you are running your agent as inetd. If you are running your agent as a daemon, select CSI_REFRESH_INETD=N	This option does not apply to Mac OS X.
CSI_NICE=10 Keep the default value	Sets the nice value for the agent listener process.

Installation Options with Default Values	Description
CSI_CERTIFICATE_PATH=	Specifies the path to Collector Certificates. The certificates specified at this path are copied to the Agent. If your Collector Certificates are stored in an accessible location on this machine, you use this option to put the certificates in the Agent location. You should install the Enterprise Certificates so that multiple collector instances collecting from the same set of Agents is supported. If this package was copied from a collector installation, this package already contains that Collector's Enterprise Certificate.
CSI_PARENT_DIRECTORY=/opt	Specifies the parent directory of the CM Agent. The root directory of CMAgent will be CSI_PARENT_DIRECTORY/CMAgent.
CSI_PARENT_DATA_ DIRECTORY=/opt	Specifies the parent directory of the CMAgent data directory. The data directory will be CSI_PARENT_DATA_DIRECTORY/ CMAgent/data.
CSI_PARENT_LOG_ DIRECTORY=default	Specifies where agent operational log files are kept. The log directory is CSI_PARENT_LOG_DIRECTORY/CMAgent/log. The default value indicates to use these values. ■ Mac OS X: log ->private/var/log/CMAgent/log
CSI_KEEP_CSIINSTALL=N Recommend keeping default value.	After a successful installation, the temp installation directory CSIInstall is deleted. To keep this installation directory, set this parameter to Y.

Manually Uninstall the Mac OS X Agent

When you install the Agent, an uninstall file, UninstallCMAgent, is automatically created in <path>/CMAgent/uninstall. You use the file to manually uninstall the Agent from the managed machine.

The uninstall reverses all changes made by installation. However, the installation log files are retained in <AgentRoot>/install. <AgentRoot> defaults to the CMAgent directory that was created during installation.

Prerequisite

Determine if you want to save a copy of the configuration file for use on other machines. If you do, copy csi.config, the file that contains all of the custom configuration settings, to a secure location. The file is located in <path>/CMAgent/install.

Procedure

1. Navigate up one level from the uninstall directory in the CMAgent directory.
2. Run the # ./uninstall/UninstallCMAgent command to uninstall the Agent.

What to do next

After you run UninstallCMAgent, delete the remaining the CMAgent directory before you install a new Agent.

Collect Mac OS X Data

When the Mac OS X machines are licensed and the Agent is installed, you collect data from those machines.

Collecting data from machines adds the collected machine information to the VCM database and makes the machine data available for reporting, running compliance, and other management options. The collection process for Mac OS X collection is similar to other collections, including Windows, except that you select Mac OS X data types during the collection instead of Windows data types.

Prerequisites

- License the target machines. See "License Mac OS X Machines" on page 124.
- Install the Agent on the target machines. See "Install the Agent on Mac OS X Machines" on page 124.

Procedure

1. On the toolbar, click **Collect**.
2. On the Collection Type page, select **Machine Data** and click **OK**.
3. On the Machines page, select the machines from which you are collecting data and click **Next**.
4. On the Data Types page, configure the collection and click **Next**.
   a. Select the **Select All** check box.
   b. Select **Use default filters**.
5. On the Important page, verify that there are no conflicts with previously scheduled or running jobs, and click **Finish**.

   The amount of time the first collection requires is determined by the number of machines and network connectivity.
6. Click Administration and select **Job Manager > History > Instant Collections > Past 24 Hours** to determine if the collection finished.

What to do next

- Review your collected data. See "Mac OS X Collection Results" on page 131.

Collected Mac OS X Data Types

The collected Mac OS X data types you can collect include related UNIX/Linux and specific Mac OS X data types.

- Custom Information - subset of CITs
- Environment Settings - Properties
- File System - File Structure
- IP Information - General
- IP Information - Routing
- IP Information - Interfaces (IF)
- IP Information - Open Ports
- Machines - General
- Machines - Power Management
- Processes - launchctl

- Security - Users > Current
- Security - Users > Information
- Security - Groups
- Properties files (.plist)
- System Logs > syslog events

Mac OS X Collection Results

Mac OS X data is displayed in VCM and is available for several management actions.

The displayed data is only as current as the last time you collected the data.

Option	Description
Console	Displays dashboards and reports based on collected data. You use the Console to view data relevant to day-to-day operations, troubleshooting, and analysis. The displayed data is based on the collected Mac OS X data types. See the online help for a list of currently collected data types. To view the dashboards, click **Console** and select **Dashboards > UNIX**. To view the summary reports, click **Console** and select **UNIX tab > Operating System > Machines > General**. You can view the data in a summary report or data grid format.
Reports	Runs pre-configured VCM reports or create custom reports. Reports are run against currently collected data. Depending on the volume or complexity of the data requested in a report, it may take time to generate the report. Refer to the online help for information about scheduling and disseminating reports. To use the reporting options, click **Reports** and select **Machine Group Reports > UNIX**.
Compliance	Determines if the collected data from target machines meets specified compliance values, and allows you to run compliance remediation actions. To run a compliance check, click **Compliance** and select **Machine Group Compliance** and follow the steps described in the online help to create rule groups, rules, filters, and templates.
Patching	Assesses target machines to determine if the machines have the most current patches. If the patches are not yet installed, you can install the latest patches on the target machines. To assess and patch machines, select **Patching**, and then select your target operating system.

Discover, Configure, and Collect Oracle Data from UNIX Machines

To manage your Oracle instances, you must discover or add the instances, modify the configuration values, and collect management view data from the instances.

An Oracle instance consists of shared memory structures and background processes that run the Oracle database. When you use VCM to collect Oracle management view data from multiple instances, you can run compliance and reports to ensure that all your instances are configured as expected.

Prerequisites

Add, license, and install the Agent on the Oracle instance host Solaris machines. See "Discover, License, and Install UNIX/Linux Machines" on page 111.

Procedure

1. "Discover Oracle Instances" on page 132

   To discover Oracle instances, you run a collection on supported UNIX/Linux machines where Oracle is installed. The Oracle instance discovery process is based on data you collect from the `oratab` file on managed Solaris machines on which Oracle is installed.

2. "Edit Oracle Instances" on page 133

   You edit Oracle instance configuration to modify the discovered or added values for Oracle Home, Oracle Software Owner, DBA Group, and Oracle Collection User.

3. "Collect Oracle Data" on page 137

   To collect Oracle data, you must collect the Oracle data types from the machines hosting the Oracle instances.

Continuous Oracle instance management is based on the latest data you collect from target instances. You can view data and run actions, such as reports or compliance, based on the collected data. See "Oracle Collection Results" on page 138.

Discover Oracle Instances

To discover Oracle instances, you run a collection on supported UNIX/Linux machines where Oracle is installed. The Oracle instance discovery process is based on data you collect from the `oratab` file on managed Solaris machines on which Oracle is installed.

Prerequisites

Add, license, and install the Agent on the Oracle instance host Solaris machines. See "Discover, License, and Install UNIX/Linux Machines" on page 111.

Procedure

1. On the toolbar, click **Collect**.
2. On the Collection Type page, select **Machine Data** and click **OK**.
3. On the Machines page, select the machines hosting the Oracle instances, select **Do not limit collection to deltas**, and click **Next**.
4. On the Data Types page, configure the collected data types and click **Next**.
   a. Expand the UNIX data type.
   b. Select **Machines - General** and **Oracle - Management Views**.
   c. Select **Use default filters**.
5. On the Important page, verify that there are no conflicts with previously scheduled or running jobs, and click **Finish**.

   The amount of time the first collection requires is determined by the number of machines and network connectivity.
6. Click **Administration** and select **Job Manager > History > Instant Collections > Past 24 Hours** to determine if the collection completed successfully.

What to do next

- Click **Administration** and select **Machines Manager > Additional Components > VCM for Oracle** and verify that the discovered configuration information is correct and that it includes an Oracle Collection User. If the information about the instance does not include a valid Oracle Collection User value, see "Edit Oracle Instances" on page 133. If the instance is not included in the data grid, see "Add Oracle Instances" on page 134.
- If VCM discovered your Oracle instances and the Oracle Collection User account is correctly configured, collect data from the target instances. See "Collect Oracle Data" on page 137.

Edit Oracle Instances

You edit Oracle instance configuration to modify the discovered or added values for Oracle Home, Oracle Software Owner, DBA Group, and Oracle Collection User.

To collect from Oracle instances, the target instances must have a configured Oracle Collection User created on the instance.

Prerequisites

- Add, license, and install the Agent on Solaris machines hosting Oracle instances. See "Discover, License, and Install UNIX/Linux Machines" on page 111.
- Collect from the target Solaris machines using the Machines - General and Oracle - Management Views data types. The collection process discovers Oracle instances from the `oratab` file on Solaris machines. See "Discover Oracle Instances" on page 132.
- Verify that the collected configuration information is correct and that it includes an Oracle Collection User. Select **Administration > Machines Manager > Additional Components > VCM for Oracle** and review the data grid values. If the instance is not in the data grid, add the instance. See "Add Oracle Instances" on page 134. If the information about the instance does not include a valid Oracle Collection User value, edit the instance to update the configuration information.

Procedure

1. Click **Administration**.
2. Select **Machines Manager > Additional Components > VCM for Oracle**.
3. Select the target instances and click **Edit**.
4. On the Select Machines page, verify that the target Oracle instance machines are in the selected machines list and click **Next**.
5. On the Configuration Values page, configure the missing or incorrect values.

a. Type the configuration values.

Option	Description
Oracle Home	File path to the location of the Oracle software for the Oracle instance (user-defined).
Oracle SW Owner	User account that owns the Oracle software for the Oracle instance (user-defined).
DBA Group	Database administrator group account for the Oracle instance.
Oracle Collection User	User account that VCM uses to collect from the Oracle instance.

b. Select **Configure Oracle Collection User for the Added Instance** to create the OS-authenticated Oracle collection user on the target Oracle instances.

If you do not select this option, you must create the Oracle Collection User using either the Config User action or the Install Oracle Collection Account remote command. See the online help for complete information.

c. Click **Next**.

6. On the Important page, click **Finish**.
7. If you selected the Configure Oracle Collection User for the Added Instance option, on the Select Oracle instances page, add the target machines to the selected list and click **Next**.
8. On the Schedule page, select **Run Action now** and click **Next**.
9. On the Important page, click **Finish**.

What to do next

- If your target Oracle instance is Oracle 10g, you must set user permissions. See "Grant Permissions for the Oracle Collection User Account on Oracle 10g" on page 136.
- To begin managing your Oracle instances, you must collect data from the target instances. See "Collect Oracle Data" on page 137.

Add Oracle Instances

Adding Oracle instances identifies host Solaris machines and provides the Oracle SID, Oracle Home, Oracle Software Owner, DBA Group, and Oracle Collection User for the added instances.

You add Oracle instances if the collection of the Oracle instances from the host machines does not retrieve Oracle Home, Oracle SID and Oracle Software Owner from the `oratab` file on host machines.

Prerequisites

- Add, license, and install the Agent on Solaris machines hosting Oracle instances. See "Discover, License, and Install UNIX/Linux Machines" on page 111.
- Collect from the target Solaris machines using the Machines - General and Oracle - Management Views data types. The collection process discovers Oracle instances from the `oratab` file on Solaris machines. See "Discover Oracle Instances" on page 132.

Procedure

1. Click **Administration**.
2. Select **Machines Manager > Additional Components > VCM for Oracle**.
3. Click **Add**.
4. On the Select Machines page, add the target Oracle instance machines to the selected machines list and click **Next**.
5. On the Configuration Values page, add instances.
   a. Type the configuration values.

Option	Description
Oracle SID	(Add only. Not available for editing.) Name or system ID of the Oracle instance, used to identify a particular database on a machine. Each database on a machine must have a unique SID.
Oracle Home	File path to the location of the Oracle software for the Oracle instance (user-defined).
Oracle SW Owner	User account that owns the Oracle software for the Oracle instance (user-defined).
DBA Group	Database administrator group account for the Oracle instance.
Oracle Collection User	User account that VCM uses to collect from the Oracle instance.

   b. Select **Configure Oracle Collection User for the Added Instance** to create the OS-authenticated Oracle collection user on the target Oracle instances.

      If you do not select this option, you must create the Oracle Collection User using either the Config User action or the Install Oracle Collection Account remote command. See the online help for complete information.

   c. Click **Add**.

   d. Continue adding configurations to apply to the selected machines or click **Next**.
6. On the Important page, click **Finish**.
7. If you selected the Configure Oracle Collection User for the Added Instance option, on the Select Oracle instances page, add the target machines to the selected list and click **Next**.
8. On the Schedule page, select **Run Action now** and click **Next**.
9. On the Important page, click **Finish**.

What to do next

- If your target Oracle instance is Oracle 10g, set user permissions. See "Grant Permissions for the Oracle Collection User Account on Oracle 10g" on page 136.
- To begin managing your Oracle instances, collect data from the target instances. See "Collect Oracle Data" on page 137.

Create the Oracle Collection User Account with the Config User Action

You can create an OS-authenticated Oracle collection user account on target Oracle instances from VCM. This action allows you manage the collection user account from VCM rather than managing the account in each Oracle instance. VCM must have the appropriate Oracle database access to collect data from Oracle instances. VCM uses the Oracle Collection User account to connect to the Oracle database and collect Oracle data.

Prerequisites

Verify that the Oracle instance is added to VCM. See "Add Oracle Instances" on page 134.

Procedure

1. Click **Administration**.
2. Select **Machines Manager > Additional Components > VCM for Oracle**.
3. Click **Config User**.
4. On the Select Machines page, add the target Oracle instances to the selected instances list and click **Next**.
5. On the Schedule page, select **Run Action now** and click **Next**.
6. On the Important page, click **Finish**

What to do next

If your target Oracle instance is Oracle 10g, you must set user permissions. See "Grant Permissions for the Oracle Collection User Account on Oracle 10g" on page 136.

Grant Permissions for the Oracle Collection User Account on Oracle 10g

For Oracle 10g installations, you must give the Oracle Collection User accounts read/execute permission to the required directories and files in Oracle Home.

By default, Oracle 10g has the permissions set to prevent users who are not part of the Oracle DBA Group from accessing and running files in the Oracle Home directory. Oracle Collection User accounts do not typically belong to the Oracle DBA Group and must be granted permissions on the required files.

Prerequisites

Verify you added VCM-created Oracle Collection User accounts to Oracle instances. See "Create the Oracle Collection User Account with the Config User Action" on page 136.

Procedure

1. On the Oracle instance, run `chmod o+rx <top level oracle install>` to grant permission for the Oracle Collection User on the required Oracle directories.

   For example, `/opt/oracle`, `/oracle`, and so on.

2. Run `chmod o+rx <top level oracle install>` for every directory level from the top level install down to `$ORACLE_HOME`.

   For example, if the top level is `/oracle` and `$ORACLE_HOME` is `/oracle/app/product/10.20.0/db_1`, then these are the required files.

   ```
   chmod o+rx /oracle/app
   ```

   ```
   chmod o+rx /oracle/app/product
   ```

```
chmod o+rx /oracle/app/product/10.20.0

chmod o+rx /oracle/app/product/10.20.0/db_1
```

3. Verify the `$ORACLE_HOME` environment variable is set and update the mode for these files.

```
chmod o+rx $ORACLE_HOME

chmod o+rx $ORACLE_HOME/jdbc

chmod o+rx $ORACLE_HOME/jdbc/lib

chmod o+rx $ORACLE_HOME/ldap

chmod o+rx $ORACLE_HOME/ldap/mesg

chmod o+r $ORACLE_HOME/ldap/mesg/*

chmod o+rx $ORACLE_HOME/network

chmod o+rx $ORACLE_HOME/network/admin

chmod o+rx $ORACLE_HOME/sqlplus

chmod o+rx $ORACLE_HOME/sqlplus/mesg

chmod o+r $ORACLE_HOME/sqlplus/mesg/sp1us.msb

chmod o+r $ORACLE_HOME/sqlplus/mesg/sp2us.msb

chmod o+rx $ORACLE_HOME/nls

chmod o+rx $ORACLE_HOME/nls/data

chmod o+r $ORACLE_HOME/nls/data/lx1boot.nlb

chmod o+r $ORACLE_HOME/nls/data/*

chmod o+rx $ORACLE_HOME/oracore

chmod o+rx $ORACLE_HOME/oracore/zoneinfo

chmod o+r $ORACLE_HOME/oracore/zoneinfo/timezlrg.dat
```

Collect Oracle Data

To collect Oracle data, you must collect the Oracle data types from the machines hosting the Oracle instances.

Prerequisites

Verify that the Oracle instances are added to VCM and correctly configured. See "Edit Oracle Instances" on page 133.

Procedure

1. On the toolbar, click **Collect**.

2. On the Collection Type page, select **Machine Data** and click **OK**.
3. On the Machines page, select the Solaris machines hosting the Oracle instances, select **Do not limit collection to deltas**, and click **Next**.
4. On the Data Types page, configure the collected data type.
   a. Expand the Unix data type.
   b. Select **Oracle - Management Views**.
   c. Select **Use default filters**.
   d. Click **Next**.
5. On the Important page, verify that there are no conflicts with previously scheduled or running jobs, and click **Finish**.

   The amount of time the first collection requires is determined by the number of machines and network connectivity.

What to do next

- Select **Administration > Job Manager > History > Instant Collections > Past 24 Hours** to determine if the collection completed successfully.
- Review collected data and manage your Oracle instances. See "Oracle Collection Results" on page 138.

Oracle Collection Results

You use the collected Oracle data to manage your Oracle instances. The data is available for several management actions.

The displayed data is only as current as the last time that you collected the data.

Option	Description
Console	Displays security information for users, roles, privileges, configuration settings, and database parameters for Oracle instances. The data in these views is collected from views in each Oracle instance on supported Solaris machines. To view the collected data, click **Console** and select **Enterprise Applications > Oracle > Management Views**.
Compliance	Determines if the collected data from target machines meets specified compliance values. To run compliance checks, click **Compliance** and select **Machine Group Compliance** and follow the steps described in the online help to create rule groups, rules, filters, and templates.
Reports	Creates custom Oracle reports based on collected Oracle management views data. Reports are run against currently collected data. Depending on the volume or complexity of the data requested in a report, it might take time to generate the report. See the online help for information about scheduling and disseminating reports. To create Oracle reports, click **Reports** and select **Machine Group Reports**.

Customize VCM for your Environment

Customization of your environment is essential to fine-tune the visibility of configuration information so that the policies you develop and the actions you take are appropriate for your IT infrastructure.

Create a machine group structure that matches the organization of the machines in your environment. With these machine groups, you can manage specific machines in your environment such as all SQL Servers in a particular location. You can apply specific changes or create roles and rules for those machines independently from other machines in your environment. This approach ensures that you can restrict access to critical machines to the appropriate users with rights to VCM.

You can customize the following options for your environment.

- **Alerts:** Define the objects and types of changes that you are alerted to when they are detected in VCM. For example, you can set an alert to notify you if a registry setting changes in your environment.
- **Collection Filters and Filter Sets:** Use collection filters to specify the data to collect from the VCM managed machines. A default collection filter is provided for each data type. You can add custom collection filters that are specific to your enterprise. You can apply filters during instant collections and scheduled collections if the filters are included in a filter set. After you create collection filters, organize them into filter sets. You can create specific filter sets or filter set groups for different machine groups. You can apply filter sets during instant collections or scheduled collections.
- **Compliance Templates and Rule Groups:** Use compliance templates and rule groups to define specific settings and verify whether or not the machines match those criteria. VCM provides prepackaged templates and rules to check the compliance of your machines with regulatory, industry, and vendor standards. VMware provides additional compliance packages that you can import into VCM.
- **Reports:** Create and print tailored reports of information that does not appear in VCM. VCM provides prepackaged reports that you can run after you collect data from your VCM managed machines.
- **Roles and Rules:** VCM roles and access rules work together to control user access to VCM. For example, you can create a role that allows a user to view all data, but not make changes to the environment. You can create a role to run certain reports or a role that allows unlimited access to a single machine group. Refer to the online Help about User Manager for more information.

  The VCM Change Restricted role limits users from making certain changes in your environment. See "Understanding User Access" on page 71.

For more information, see the online help. For information to import additional compliance packages into VCM, see Import/Export and Content Wizard.

For questions about VCM, contact VMware Technical Support.

How to Set Up and Use VCM Auditing

The VCM Auditing capability tracks all changes in the security aspects of VCM. Security-related events are written to the Windows Event Log, which is stored on the Collector, and is independent of the VCM application. The format of the event log prohibits any modifications to the recorded entries, which makes it a secure and tamper-proof auditing record of changes in security.

When you perform an action in VCM that affects security, and the auditing setting that corresponds to that change is enabled, the event is written to the event log. Examples of VCM actions that cause events to be written to the event log include user log on and log off, session timeouts, changes in managing users, changes to passwords and administration settings, changes in network accounts and authority, collection requests, and service and registry changes.

NOTE Only users who are assigned and logged in with the Admin role can enable or disable Auditing settings.

1. To view the VCM Auditing settings, click **Administration** and select **Settings > General Settings > Auditing**.
2. To change an auditing setting, highlight a setting and click **Edit Setting**.

   When you change an auditing setting, the VCM Auditing data grid displays the user's name in the Last Modified By column.

What to do next

For details about the Auditing settings and the Windows Event Log, see the online help.

8 Getting Started with VCM for Virtualization

VCM collects virtualization configuration information for virtual machine hosts, their guest operating systems, VMware vCenter Servers™, and VMware vCloud Director vApps.

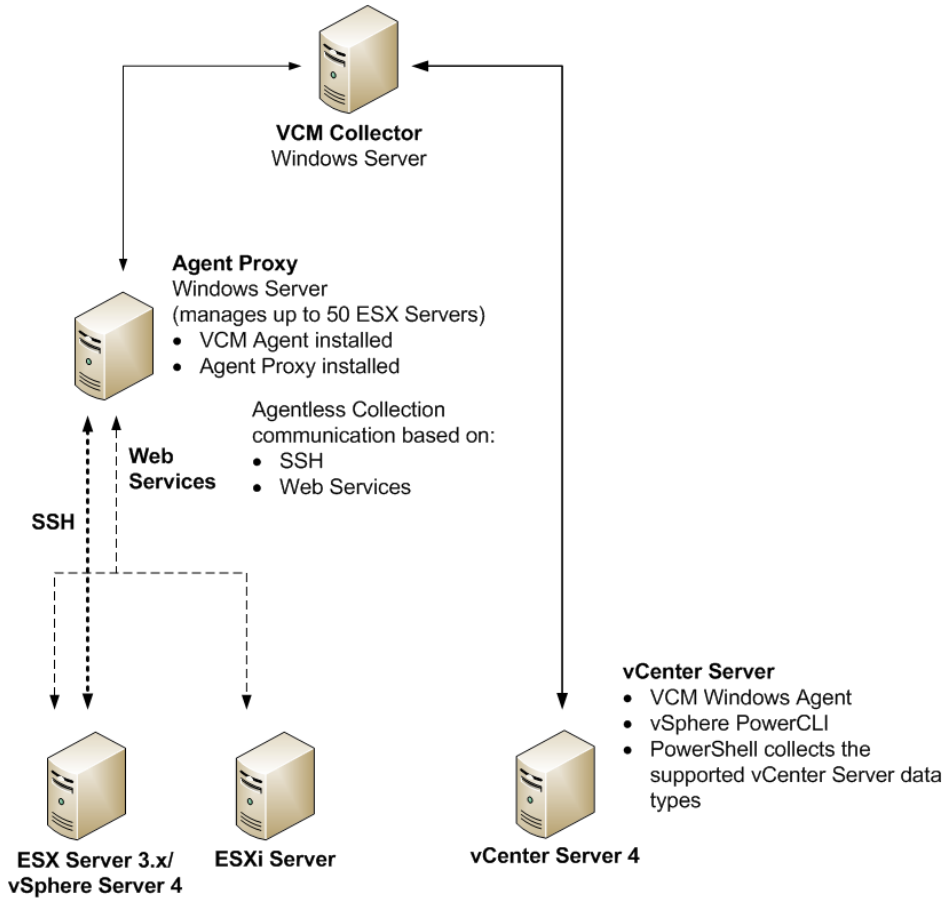
The collected data is displayed in the Console slider under the Virtual Environments node. The information is organized in a logical grouping of the configurations of virtual machine hosts, virtual machine guest operating systems, and vCenter servers. Using the grouping, you can view your virtual environments at an enterprise level based on collected data.

Virtual Environments Configuration

To collect virtual environment data from VMware ESX® and VMware ESXi® servers and vCenter servers, you must configure different communication options for each target source.

- To collect ESX and ESXi data, you use an Agent Proxy rather than installing the VCM Agent directly on the ESX and ESXi servers.
- To collect data from VirtualCenter and vCenter servers, the VCM Agent is installed on the Windows machines running vCenter server.

Figure 8–1. Virtual Environments Configuration Diagram



ESX/ESXi Server Collections

When collecting from ESX and ESXi servers, you must configure at least one VCM Agent Proxy machine. You can configure the Collector as the Agent Proxy or configure standalone Agent Proxy machines. The Collector communicates with the Agent Proxy and the Agent Proxy then directly communicates with the ESX and ESXi servers using SSH and/or Web Services for necessary data collection actions. The data is processed by the Agent Proxy and relayed to the Collector.

The Agent Proxy machine must be a Windows server that meets the minimum hardware and software requirements specified in the *VCM Hardware and Software Requirements Guide*. A single Agent Proxy machine supports up to 50 ESX or ESXi servers.

VCM Support of ESXi

VCM supports collecting VM guest operating system and VM host data from ESXi machines. ESXi does not support SSH communication. Therefore, you cannot run UNIX remote commands or collect UNIX and Linux data types data on ESXi machines. Only Web service settings are required for ESXi machines. The License VM Host wizard for the ESXi machines includes SSH settings, but you should not configure them.

IMPORTANT When you collect data from ESXi servers, attempting to collect data other than VM hosts or VM guest operating data from the ESXi servers results in a collection failure. This restriction includes collection filters for ESX3.x and vSphere4 that are supplied with VCM. Running such collections on all the All VM Hosts Machine fails on the ESXi machines.

---

vCenter Server Collections

When collecting data from vCenter Server, you must license the Windows machine running the vCenter Server and install a VCM Agent (version 5.4 or later), PowerShell, and vSphere PowerCLI. The Agent runs the vCenter Server collection by using vSphere PowerCLI to access the vSphere API on vCenter server. The data is relayed to the Collector and added to the database.

vCloud Director vApp Virtual Machines Collections

To accommodate how vCloud Director manages vApps, which can include duplicate names, IP addresses, and MAC addresses, VCM collects and displays internal and external IP address information, internal machine name information, and vCenter machine name information collected directly from vCloud Director. Based on the collected data, you determine how VCM constructs a unique virtual machine name and specify which IP address to use based on the network address translation (NAT) mapping level.

To identify the vCloud Director virtual machines, you configure discovery rules that analyze data collected from the vCloud Director REST API and use the vApp virtual machine information to add new virtual machines to VCM. After installing the Agent and licensing the virtual machines, you manage the new machines based on their operating systems. The machines appear in VCM based on your configured naming convention.

Configure vCenter Server Data Collections

Collecting vCenter server data is based on a process that extends beyond the standard Windows collection. The configuration of the process has several prerequisites. When the prerequisites are met, data is collected from vCenter Server by using default collection filters.

Procedure

1. "Configure vCenter Server Collection Prerequisites" on page 143

   The vCenter Server collection prerequisites prepare your environment for collecting data from vCenter Servers.

2. "Collect vCenter Server Data" on page 145

   The vCenter Server collection is based on default collection filters for vCenter Host Profiles, vCenter Host Status, and vCenter Inventory.

The collected vCenter Server data appears in the Console in the Virtual Environments node. The collected vCenter Server data helps you identify and manage VM Host machines. See " vCenter Server Collection Results" on page 146.

Configure vCenter Server Collection Prerequisites

The vCenter Server collection prerequisites prepare your environment for collecting data from vCenter Servers.

1. "Configure the VCM Agent with HTTP Communication" on page 144

   Configure the VCM Agent (5.4 or later) on the vCenter server with HTTP communication. You cannot collect vCenter Server data if the Agent is not configured to use HTTP.

2. "Add vCenter Server User with Administrator Role" on page 144

   The VCM Agent Network Authority Account must be added as a vCenter Server user with an Administrator Role.

3. "Remove PowerShell v1.x from vCenter Servers" on page 144

   To collect from vCenter Servers, you must first uninstall PowerShell 1.x from those machines.

4. "Download and Install PowerShell v2.0 " on page 145

   To collect data from vCenter Servers, you must install PowerShell 2.0 on the target machines.

5. "Download and Install VMware vSphere PowerCLI" on page 145

   To collect from vCenter Servers, you must install VMware vSphere PowerCLI 4.1 or later on the target machines.

Configure the VCM Agent with HTTP Communication

Configure the VCM Agent (5.4 or later) on the vCenter server with HTTP communication. You cannot collect vCenter Server data if the Agent is not configured to use HTTP.

Prerequisites

Install the Agent (5.4 or later) on the vCenter server. See "Discover, License, and Install Windows Machines" on page 77.

Procedure

1. In VCM, click **Administration**.
2. Select **Machines Manager > Licensed Machines > Licensed Windows Machines**.
3. Select the vCenter Server machines and verify that the **Protocol** field displays HTTP.
4. If HTTP is not displayed, change the protocol.
   a. Click **Change Protocol**.
   b. On the Machines page, verify the list of selected machines and click **Next**.
   c. On the Change Protocol page, select **Switch to HTTP** and click **Next**.
   d. On the Important page, review the number of selected machines, the type of change, and click **Finish**.

You can view the status of the change protocol job in Job Manager.

Add vCenter Server User with Administrator Role

The VCM Agent Network Authority Account must be added as a vCenter Server user with an Administrator Role. See the vCenter Client online help for information about adding users to vCenter.

Remove PowerShell v1.x from vCenter Servers

To collect from vCenter Servers, you must first uninstall PowerShell 1.x from those machines. PowerShell 1.x is often installed by other applications and must be removed.

Procedure

1. On the vCenter server, go to **Add/Remove Programs**.
2. Select **Show Updates**.

   The list displays updates associated with installed programs.
3. Look for any of the following knowledge base numbers, which indicate earlier versions of PowerShell.

   Versions of v1.x prior to RC2 are MS-based installations. These versions will appear as Windows PowerShell in the programs list.

   - KB926139 - Windows PowerShell v1.0 RTM - English Language Version
   - KB926140 - Windows PowerShell v1.0 RTM - Localized Installation Package
   - KB926141 - Windows PowerShell v1.0 RTM - MUI pack
   - KB925228 - Windows PowerShell v1.0 RC2
4. Uninstall any occurrence of PowerShell v1.x.

Download and Install PowerShell v2.0

To collect data from vCenter Servers, you must install PowerShell 2.0 on the target machines.

Prerequisites

- Uninstall previous versions of PowerShell. See "Remove PowerShell v1.x from vCenter Servers" on page 144.
- Locate the PowerShell download page at `http://support.microsoft.com/kb/968929`.

Procedure

1. Download and install the appropriate version of PowerShell 2.0 included in the Windows Management Framework on the vCenter Server.
2. Reboot the vCenter Server machine.

Download and Install VMware vSphere PowerCLI

To collect from vCenter Servers, you must install VMware vSphere PowerCLI 4.1 or later on the target machines.

Prerequisites

Locate the VMware vSphere PowerCLI download page at `http://www.vmware.com/support/developer/PowerCLI/index.html`. You must be registered on the VMware Web site.

Procedure

1. Download and install VMware vSphere PowerCLI on the vCenter Server machines.

Collect vCenter Server Data

The vCenter Server collection is based on default collection filters for vCenter Host Profiles, vCenter Host Status, and vCenter Inventory.

Prerequisites

- Verify that you completed all the pre-collection prerequisites. See "Configure vCenter Server Collection Prerequisites" on page 143.
- Collect the Machines data type from the Windows machines on which vCenter Server is installed. This action identifies the machines as a vCenter Servers. See "Collect Windows Data" on page 90.

Procedure

1. Click **Collect**.
2. On the Collection Type page, select **Machine Data** and click **Next**.
3. On the Machines page, select one or more vCenter Server machines and click **Next**.
4. On the Data Types page, expand **Windows**, select the **vCenter** data type, and click **Next**.
5. On the Important page, review and resolve any conflicts and click **Finish**.

What to do next

After you collect vCenter data, the vCenter servers and any VCM-managed Host machines are automatically added to the Virtual Environments machine groups. Using the machine group, you can schedule regular collection jobs to collect vCenter data. See " vCenter Server Collection Results" on page 146.

vCenter Server Collection Results

The collected vCenter Server data appears in the Console in the Virtual Environments node. The collected vCenter Server data helps you identify and manage VM Host machines.

Option	Description
Console	View the collected vCenter data. Click **Console** and select **Virtual Environments**.

Troubleshooting vCenter Server Data Collections

If you encounter problems with vCenter collections, review the troubleshooting options.

vCenter Data Missing

Data does not appear in the vCenter server data grids.

Problem

After you collect vCenter data, the data grids do not display the new data.

Cause

The required VMware Web Services are not running on the vCenter machine

Solution

On the vCenter server machine, verify that the VMware VirtualCenter Management Web Services in running.

Configure Virtual Machine Host Collections

To manage your virtual machine hosts, ESX and ESXi servers, VCM uses an Agent Proxy rather than installing the VCM Agent directly on the ESX and ESXi machines. However, you must copy required files and certificates on the ESX and ESXi servers to manage the data collection from those machines.

After you configure the Agent Proxy, you should license, configure, and copy files. You perform the tasks first for ESX servers and then for ESXi servers.

1. "Configure the Collector as an Agent Proxy" on page 147

   The Agent Proxy machine is a Windows machine configured to communicate with ESX and ESXi servers and to remotely collect data from those servers. The Collector automatically meets the Agent Proxy requirements. You license the Collector and then collect the Machines data type.

2. "License and Configure Virtual Machine Hosts" on page 148

   License virtual machine hosts to generate a file containing machine names and settings. You use the generated file to configure the ESX and ESXi machines for management in VCM.

3. "Copy Files to the ESX/ESXi Servers" on page 150

   To import target machine information and copy the required files from VCM, you use the UNIX/ESX/vSphere Deployment Utility on your Agent Proxy machines.

4. "Collect Virtualization Data" on page 151

   An initial collection of Virtual Environments data identifies your virtual machine hosts and their guest machines.

You have several options for reviewing and using virtualization data in VCM. The data used is only as current as the last collection, and the amount of time it takes for the data to display is based on the volume or complexity of the data requested. See "Virtualization Collection Results" on page 152.

vCenter Server Collection Upgrade Considerations

A new method for collecting vCenter Server data was introduced in VCM 5.4 that is simpler to implement and manage. The older method (5.3 and earlier), implemented using Windows remote commands, has been replaced with this new method.

Data that you previously collected by using the vCenter Server remote commands is no longer available. You must recreate scheduled collections to accommodate the new method. However, previously configured compliance rules, reports, and alerts based on the previously collected data are automatically redirected to the data in the new data grids.

Configure the Collector as an Agent Proxy

The Agent Proxy machine is a Windows machine configured to communicate with ESX and ESXi servers and to remotely collect data from those servers. The Collector automatically meets the Agent Proxy requirements. You license the Collector and then collect the Machines data type.

NOTE If you manage more than fifty VM Host machines, you must use a separate Windows machine as your Agent Proxy. Moving the Agent Proxy activity to the separate machine optimizes performance. See "Configuring Standalone Agent Proxy Machines" in the online Help for more information about configuring other Windows machines as Agent Proxies.

Procedure

1. Click **Administration**.
2. Select **Machines Manager > Available Machines > Licensed Windows Machines**.
3. Determine if the Collector machine name appears in the data grid.

   If it is listed in the data grid, the machine is licensed. If it is not listed, continue with the licensing process.
4. Select **Machines Manager > Available Machines > Available Windows Machines**.
   a. Select the Collector in the data grid and click **License**.
   b. On the Machines page of the Available Machines License wizard, verify the Collector machine name is displayed in the Selected list and click **Next**.
   c. Review the Product License Details page and click **Next**.
   d. Review the Important page and click **Finish**.
   e. Select **Administration > Machines Manager > Licensed Machines > Licensed Windows Machines** to verify the Collector is now licensed.
   f. Click **Refresh** on the Console toolbar to update the displayed data.
5. Select the Collector in the Licensed Windows Machines data grid and click **Collect** on the Console toolbar.
6. On the Collection Type page, click **Machine Data** and click **OK**.
7. On the Machines page, verify the Collector machine name is displayed in the Selected list, click **Select Data Types to collect from these machines** and click **Next**.
8. On the Data Types page, expand the Windows tree and select **Machines**.
9. Select **Use default filters** and click **Next**.
10. Review the Important page and click **Finish**.

    The collection job starts. You can use the Job Manager to determine when the collection is completed.
11. When the collection is completed, select **Administration > Machines Manager > Agent Proxies** and verify the Collector machine Agent Proxy State equals Current Agent.

What to do next

License and configure the target virtual machine hosts. See "License and Configure Virtual Machine Hosts" on page 148.

License and Configure Virtual Machine Hosts

License virtual machine hosts to generate a file containing machine names and settings. You use the generated file to configure the ESX and ESXi machines for management in VCM.

All Virtualization data types are collected through Web Services communication except for the VM Logs, which are collected through SSH and only from ESX machines. Web Services must be set up on your virtual machine hosts before data can be collected.

Prerequisites

- Verify that at least one Agent Proxy machine is configured. See "Configure the Collector as an Agent Proxy" on page 147.
- License the ESX and ESXi machines as UNIX machines. See "License UNIX/Linux Machines" on page 114.
- Verify that vCenter Server data is collected. If using vCenter, the hostname in vCenter must match the configured hostname of the ESX server. It must be a Fully-Qualified Domain Name (FQDN), not an IP address. If the name does not match, you must manually add the machine. See the online Help.

Procedure

1. Click **Console**.
2. Select **Virtual Environments > vCenter > Inventory > Manage VM Hosts**.
3. Add the machines to be configured to the lower grid and click **Next**.

   The selected machines will use the same Agent Proxy and the same SSH and Web Services settings.
4. Configure the settings on the Agent Proxy and Communication Setting page.

Option	Description
Agent Proxy	The configured Agent Proxy used to manage the selected VM Host machines. This option is required when you are licensing VM Hosts but optional if you are modifying the settings.
SSH Settings	Select the check box to configure the settings for your ESX machines. Configure these settings if you plan to collect VM Logs data from the managed VM Host machines. ■ **Port:** Used by VMware's Web Services SDK for the ESX server on which SSH listening. The Agent Proxy communicates with the ESX server using this port. The default port (22) is set to the default value for SSH on ESX. ■ **User ID:** Used by the Agent Proxy to communicate with the ESX server through SSH. This account must have certain permissions, for example, sudoers, defined in the installation process. Authentication for this account uses public key cryptography that was setup during the installation process.
Web Services Settings	Select the check box to configure the settings for your ESX and ESXi machines. Configure the settings to collect virtual environment data from a VM host. ■ **Port:** The port on the ESX server used by the Agent Proxy to communicate with the VMware web services interface. ■ **User ID:** The account that has access to the VMware web services interface. If you are using ESX, this account must have Administrator access to web services on the ESX server. This user ID may be different from the user ID for SSH communication, depending on whether you created different accounts during the ESX installation process. ■ **Password:** The password for the web services User ID specified above. This password is encrypted in the VCM database.

Option	Description
	■ **Confirm Password:** Retype the password. ■ **Ignore untrusted SSL Certificate:** Connection allowed even when certificates are not verified as trusted.

5. On the Important page, record the `.xml` file name.

   The file is saved to the location configured for `CMFiles$\VMHosts_Config`. The default location is `\Program Files (x86)\VMware\VCM\WebConsole\L1033\Files\VMHosts_Config`.

6. Click **Finish**.

   The machines are displayed in the Licensed VM Hosts.

What to do next

Copy the copy SSH public key file, the `csiprep.py` file, and the `csiprep.config` file to the target ESX machines. See "Copy Files to the ESX/ESXi Servers" on page 150.

Copy Files to the ESX/ESXi Servers

To import target machine information and copy the required files from VCM, you use the UNIX/ESX/vSphere Deployment Utility on your Agent Proxy machines.

For ESX machines, you import target machine information from VCM and copy the SSH public key file, the `csiprep.py` file, and the `csiprep.config` file to the target ESX machines.

For ESXi machines, you import machine information and copy the necessary Web Services settings to the target machines.

Prerequisites

- License the ESX and ESXi machines. See "License and Configure Virtual Machine Hosts" on page 148.
- Locate the UNIX/ESX/vSphere Deployment Utility file. The Deployment Utility file is located on the Collector in `C:\Program Files (x86)\VMware\VCM\Tools\DeployUtility-<version number>`.
- Consult the Deployment Utility online help when using the tool.

Procedure

1. Copy the UNIX/ESX/vSphere Deployment Utility file to the Agent Proxy machine, either a standalone Windows machine or the Collector, and unzip the file.
2. Double-click `DeployUtil.exe` to start the Deployment Utility.
3. Click the **ESX/vSphere Configuration** tab.
4. Click **File > Open**.
5. Browse to the location of the virtual machine hosts configuration file generated when you licensed and configured the virtual machine hosts.

   The default location on the Collector is `\Program Files (x86)\VMware\VCM\WebConsole\L1033\Files\VMHosts_Config`.

6. Select the `.xml` file and click **Open**.

   The machine information in the `.xml` file is imported into the **ESX Server Settings** table on the **ESX/vSphere Configuration** tab with the settings you defined in VCM.

7. Select a configuration option:

Option	Description
Configure ESX 3.x Servers	Configures the SSH certificate, the csiprep.py file, the csiprep.config file, and passes the SSH and Web Services user information to the target machines.
Configure ESXi Servers	Passes the Web Services to the target machines

8. (Optional) Configure the default server location.

   The following settings are automatically configured to the default server locations. If you need to change the paths, click the ellipsis button.

   - SSH Public Key file (ESX 3.x only)
   - Log Files Location
   - `csiprep.py` File (ESX 3.x only)
   - `csiprep.config` File (ESX 3.x only)

9. (Optional) Configure the VCM user name and password.

   If you configured the settings in VCM and want to modify them, use the following options or manually change the values in the ESX Server Settings table. For more information about the settings, see the Deployment Utility online Help.

   - Use the same user name for both SSH and Web Services collections (ESX 3.x only)
   - Use the same password for all WebServices Users
   - Apply the same user names and passwords to all ESX servers

10. Click **Configure**.

    All the machines where the **Configure** check box is selected now have the same version of the files copied to the location specified in the Remote Path field in the table. If no path is specified, the files are copied to the `/tmp` directory.

What to do next

Collect data from the target virtual machine hosts. See "Collect Virtualization Data" on page 151.

Collect Virtualization Data

An initial collection of Virtual Environments data identifies your virtual machine hosts and their guest machines.

Procedure

1. On the Portal toolbar, click **Collect**.
2. Select either your ESX or ESXi Servers.

   To avoid configuration conflicts, do not select both for one action. The selected machines are displayed in the Selected list.

3. Click **Select Data Types to collect from these machines** and click **Next**.

4. For ESX machines only, on the Collection Wizard Data Type page, expand the UNIX node and select the **Machines - General** data type.
5. Expand the Virtualization node and select the **VM Hosts** and **VM Guests** data types.
6. Click **Use default filters** and click **Next**.
7. Click **Finish**.

Monitor the collection job in Job Manager. When the collection is completed, the data is available for reports and compliance assessments.

What to do next

Review the collected data in the Console, run reports, configure alerts, and use the machine groups. See "Virtualization Collection Results" on page 152.

Virtualization Collection Results

You have several options for reviewing and using virtualization data in VCM. The data used is only as current as the last collection, and the amount of time it takes for the data to display is based on the volume or complexity of the data requested.

Option	Description
Console	View ESX and ESXi server information. Click **Console** and select **UNIX (tab) > Operating System > Machines > General**. View VM Host and Guest Summary information. Click **Console** and select **Dashboards > Virtual Environments**.
Reports	View reports related to your Virtual Environments. Click **Reports** and select **Machine Group Reports > Virtual Environments**. View reports for ESX/ESXi Servers. Click **Reports** and select **Machine Group Reports > UNIX**.
Administration	Use VM Host, VM Guest, and Virtual Environments vCenter machine groups. Click **Administration** and select **Machines Manager > Machine Groups > All Machines**.
	Configure alerts. Click **Administration** and select **Alerts**.

Configure vCloud Director vApp Virtual Machines Collections

Using VCM, you collect vCloud Director data so that you can identify and manage vApp virtual machines.

To accommodate how vCloud Director manages vApps, which can include duplicate names, IP addresses, and MAC addresses, VCM collects and displays internal and external IP address information, internal machine name information, and vCenter machine name information collected directly from vCloud Director. Based on the collected data, you determine how VCM constructs a unique virtual machine name and specify which IP address to use based on the network address translation (NAT) mapping level.

To identify the vCloud Director virtual machines, you configure discovery rules that analyze data collected from the vCloud Director REST API and use the vApp virtual machine information to add new virtual machines to VCM. After installing the Agent and licensing the virtual machines, you manage the new machines based on their operating systems. The machines appear in VCM based on your configured naming convention.

Prerequisites

Review how network address translation is used in your vCloud Director environment. See "Network Address Translation and vCloud Director vApp Discovery Rules" on page 153.

Procedure

1. "Generate vCloud Director Collection Credentials" on page 155

   To collect vCloud Director data, you must generate encrypted user credentials that the collection filters use to access vCloud Director.

2. "Create vCloud Director Data Collection Filters" on page 156

   For each of your vCloud Director instances, you clone the custom information collection filter template to create a unique collection filter for each instance.

3. "Collect vCloud Director Data" on page 158

   You collect the vCloud Director data using the collection filters configured for each vCloud Director instance. You must run the collection against the Collector, not the vCloud Director.

4. "Discover vCloud Director vApp Virtual Machines" on page 158

   To begin managing the vCloud Director vApp virtual machines, you create and run a VCM discovery rule. The rule runs against the collected vCloud Director data in the VCM database.

The vCloud Director data is collected using a collection filter with the Custom Information (Win) data type. The collected data appears in the Console. The discovered vApp virtual machines appear in Administration. After you license the virtual machines and install the Agent, you manage them based on their operating system.The collected vCloud Director data appears in the Console. The discovered virtual machines appear on Administration. After you license the virtual machines and install the Agent, you manage them based on their operating system. See "vCloud Director Collection Results" on page 162.

Network Address Translation and vCloud Director vApp Discovery Rules

To configure the connection string when creating a vCloud Director virtual machines discovery rule, you must know how network address translation (NAT) is implemented in your vCloud Director instances.

The vCloud Director administrator configures the NAT mapping. How the virtual machines are configured with NAT and where VCM is in the network determines the connection string that VCM uses to communicate with the virtual machines.

vCloud Director 1.0 and 1.5 support a variety of vApp network configurations. VCM supports these scenarios.

- VCM is located in the vApp with the virtual machines that it is managing.
- The vApp has a direct connection to the org network.
- The vApp has a direct connection to the external network.
- The vApp has a one IP address to one IP address NAT connection to the organization network with direct connection to the external network.
- The vApp has a one IP address to one IP address NAT connection to the organization network with a one IP address to one IP address NAT connection to the external network.
- The vApp has a direct connection to the organization network with one IP address to one IP address NAT connection to the external network.

VCM does not support one IP address to many IP addresses NAT mapping for vCloud Director vApp virtual machines.

To determine the connection string to use when discovering the vCloud Director virtual machines, you must know where VCM is located in the network and how NAT is implemented.

Table 8–1. Determining the Connection String Based on Network Configuration

Location of VCM or the Proxy Server on the Network	External Network	Organization Network	Discovery Rule Connection String
In the managed vApp	NA	NA	Internal IP
On Org Network	NA	Direct connection	None (use DNS) or Internal IP
On Org Network	NA	NAT at vApp level	vApp External IP
On External Network	Direct Connection	Not connected or direct connection	Internal IP
On External Network	Direct from Organization	NAT at vApp level	vApp External IP
On External Network	NAT at Org level	The vApp level IP is collected from vCloud Director, but it is not used for the VCM connection.	Org External IP

After you collect the vCloud Director data, you can view the internal and external IP addresses in the virtual machine's network information.

Best Practice

VCM cannot use DCOM to communicate with vCloud Director vApp virtual machines across NAT mapped networks.

In a NAT mapped network environment, your best practice is to install the Agent on the vApp template machines. You must manually install the Agent with the HTTP mode enabled, but you must not collect data from these template machines. Collecting from the template machines generates machine-specific information that will later cause the virtual machines created from the template to run incomplete collections.

If you discovered NAT mapped vApp virtual machines that do not have the Agent preinstalled on the templates from which they were created, you must manually install the Agent. The Agent must be installed with the HTTP protocol enabled. See "Manually Install the VCM Windows Agent" on page 84.

Generate vCloud Director Collection Credentials

To collect vCloud Director data, you must generate encrypted user credentials that the collection filters use to access vCloud Director.

You generate encrypted strings of the user name and the password to use when configuring the Windows Custom Information filter for the vCloud Director collection filter. You create the credentials for the VCM Collector. If you use one Collector to manage all your vCloud Director instances, you create the encrypted user credentials once. If you have two Collectors managing different vCloud Director instances, you create credentials on each managing Collector and use those credentials on the vCloud Director instances from which you are collecting data.

Prerequisites

- Determine whether you are collecting vCloud Director data at the system (Provider) level or the organization level and have the appropriate vCloud Director user name and password available. If you use a system login, data is collected for all organizations. If you use an organization login, only data for that organization is collected.
- Ensure that you have the user name and password for the user that runs the Collector service. You can log in as the user or run PowerShell as the user.

Procedure

1. Log in to the VCM server as the user that runs the Collector service.
2. Open a PowerShell Console.
3. Run the `$sspw = Read-Host "Enter data to encrypt" -AsSecureString` command.
4. At the `Enter data to encrypt` prompt, type the user login that you are encrypting.

   For example, [login_name]@system or [login_name]@[org].
5. Run the `ConvertFrom-SecureString -SecureString $sspw` command.

   Powershell generates the encrypted string.
6. Copy the string to a text editor and remove the carriage returns.
7. Keep or save the encrypted user name in a text file.
8. In the PowerShell Console, run the `$sspw = Read-Host "Enter data to encrypt" -AsSecureString` command.
9. At the `Enter data to encrypt` prompt, type the password for the user login.
10. Copy the string to a text editor and remove the carriage returns.
11. Save the encrypted password in a text file for later use.

What to do next

Create and run a collection filter for each vCloud Director instance. See "Create vCloud Director Data Collection Filters" on page 156.

Create vCloud Director Data Collection Filters

For each of your vCloud Director instances, you clone the custom information collection filter template to create a unique collection filter for each instance.

Prerequisites

- Ensure that you have the URLs for vCloud Director instances from which you are collecting.
- Ensure that the trusted VCM certificates are installed on vCloud Director instances from which you are collecting.
- Ensure that you have the necessary encrypted credentials. See "Generate vCloud Director Collection Credentials" on page 155.

Procedure

1. Click **Administration**.
2. Select **Collection Filters > Filters**.
3. Select the **Custom Info Win 10: vCloud Director Template** and click **Clone**.
4. On the Name and Description page, type a new name for the filter and click **Next**.

   To identify the filter, include the name of the vCloud Director from which you are collecting.
5. On the Data Type page, click **Next**.

You cannot modify any values.

6. On the Windows Custom Information Filter page, configure the script with your vCloud Director information and click **Next**.

Option	Description
Script Type	Select PowerShell v2.0 Text Output.
Output Type	Select Element Normal XML.
Timeout	Select 1800 seconds as the amount of time the Agent allows a PowerShell script to run before it ends the process.
Script	Update the vCloud Director variables in the script. ■ `$baseuri = "https://VCLOUD HOST NAME/api/v1.0"` Replace `VCLOUD HOST NAME` with your vCloud Director URL. The URL must match the machine name in the issued certificate. ■ `$encrypted_user = "<encrypted user login>"` Replace the existing string with the encrypted string for the user login that you generated. ■ `$encrypted_pass = "<encrypted user password>"` Replace the existing string with the encrypted string for the user login password that you generated. ■ (Optional) `$ignore_cert_errors = $false` To ignore untrusted certificates, change the `$false` value to `$true`. The certificate of the vCloud Director URI should be trusted by the VCM Collector. VMware does note recommend ignoring untrusted certificates.
Duplicate Handling	Select **Increment** to resolve duplicate violations of duplicate path attributes in the PowerShell script.

7. On the Important page, review your changes and click **Finish**.

What to do next

Collect data from the vCloud Director instances using the collection filter. See "Collect vCloud Director Data" on page 158.

Collect vCloud Director Data

You collect the vCloud Director data using the collection filters configured for each vCloud Director instance. You must run the collection against the Collector, not the vCloud Director.

Prerequisites

- Create a vCloud Director collection filter. See "Create vCloud Director Data Collection Filters" on page 156.
- Ensure that PowerShell 2.0, which is required to run the script, is installed on the Collector.

Procedure

1. On the toolbar, click **Collect**.
2. On the Collection Type page, select **Machine Data**.
3. On the Machines page, select the options and click **Next**.
   a. Move the Collector to the Selected machines list.
   b. Select the **Select Data Types to collect from these machines** option.
4. On the Data Types page, select the options and click **Next**.
   a. In the Window tree, select **Custom Information (Windows)**.
   b. Select the **Select data filters** option.
5. On the Filters page, move the filter that you created to the lower pane and click **Next**.
6. On the Important page, resolve any conflicts and click **Finish**.

What to do next

- Review the collection jobs to determine if your collection finished. Click **Administration** and select **Job Manager > History > Instant Collections**.
- Review the collected vCloud Director data. Click **Console** and select **Console > Windows tab > Operating System > Tree View - Standard**. Expand **vCloud** to view the collected organizations, virtual data centers (VDC), vApps, virtual machines, and virtual machine network data.
- Discover the vApp virtual machines created by the vCloud Director and make them available in VCM. See "Discover vCloud Director vApp Virtual Machines" on page 158.

Discover vCloud Director vApp Virtual Machines

To begin managing the vCloud Director vApp virtual machines, you create and run a VCM discovery rule. The rule runs against the collected vCloud Director data in the VCM database.

Prerequisites

- Collect vCloud Director data. You can run the discovery only on the collected data. See "Collect vCloud Director Data" on page 158.
- Determine how NAT is used in vCloud Director network and where VCM is located in relationship to the network. See "Network Address Translation and vCloud Director vApp Discovery Rules" on page 153.

Procedure

1. Click **Administration**.
2. Select **Machines Manager > Discovery Rules**.
3. On the data grid toolbar, click **Add**.
4. On the Discovery Rules page, type a Name and Description, and click **Next**.
5. On the Discovery Method page, select **By DB Discovery** and click **Next**.
6. On the Discovery Query page, in the Discovery Query drop-down menu, select **vCloud Director Managed VMs** and click **Next**.
7. On the Discovery Query Parameters page, configure the options to use when discovering and adding the data to VCM and click **Next**.

Option	Description
Machine Name Format	Select the format used to display the virtual machine name. You can select the vCenter name for the virtual machine or select a combination of names for the virtual machine, that includes the vApp that contains the virtual machine, the vCloud Director organization, and the vCloud Director instance. With these formats, you can easily sort, group, and display the data in VCM. The composite name is limited to 128 characters. ■ **VCName:** Name of the virtual machine in vCenter. vCloud Director creates the virtual machine and generates the name of the virtual machine, which includes the machine's host name and the 10-digit identification number of the virtual machine in vCenter. This name is unique in a single vCloud Director instance. ■ **vApp:VCName:** Name of the vApp that contains the virtual machine and the name of the virtual machine in vCenter. ■ **vDC:vApp:VCName:** Name of the virtual datacenter with the vApp name and the name of the virtual machine in vCenter. ■ **Org:vDC:vApp:VCName:** Name of the vCloud Director organization with the virtual datacenter name, the name of the vApp that contains the virtual machine, and the name of the virtual machine in vCenter. ■ **Cloud:Org:vDC:vApp:VCName:** Name of the vCloud Director instance with the name of the vCloud Director organization, the virtual datacenter name, the name of the vApp that contains the virtual machine, and the name of the virtual machine in vCenter.
Machine Name Delimiter	Select a character to separate the elements of the vCloud Director hierarchy that you use as the machine name.
Domain Name	Type or select the domain in which you are managing the virtual machines.
Domain Type	Select the type of domain to which you are adding the virtual machines.
Protocol	Select the protocol by which the Collector will communicate with the Agent. If the virtual machines in the vApp use NAT mapping, you must select HTTP. If

Option	Description
	the virtual machines do not use NAT, you can use HTTP or DCOM.
HTTP Port	If you selected the HTTP protocol, you must specify the port used to communicate with the Collector. Uses the HTTP Listener on the target machine. The listener is configured to listen on the designated port. Port 26542 is the default setting. Accepted port values range from 1–65535. Other applications should not use this port.
Use a proxy server	Select **Yes** if you use a proxy server for communication between the Collector and the Agents on the virtual Windows machines. Select **No** if you do not use a proxy server or if you are managing UNIX/Linux machines. If the machines you add are Windows machines, you can select a proxy server for communication between the Collector and the Agents on managed machines that are located on the other side of a proxy server. The proxy server routes requests from the Collector to the Agents on managed machines. A proxy server can only be used with Windows HTTP agents.
Connection String	Select the IP address to use when communicating with the virtual machines. This address can differ from the address that resolves by machine name from DNS or other name resolution systems. Use this address when VCM must contact a vApp virtual machine through a Network Address Translation (NAT) address, or when DNS available to the Collector cannot resolve the vApp virtual machines. The connection string depends on the type and level at which NAT mapping is configured. ■ **None (use DNS):** The Collector resolves the IP address to the virtual machine based on the configured name resolution mechanisms. For example, DNS or Hosts. ■ **Internal IP:** The IP address that the virtual machine has in the vApp. ■ **vApp External IP:** The IP address external to the vApp addresses of the virtual machines that are configured with NAT at the vApp level. ■ **Org External IP:** The IP address external to the organization addresses of the virtual machines that are configured with NAT at the organization level or at the organization and vApp level. If NAT is implemented at the vApp and organization level, select this option.
Cloud Name Filter	To run the query against all system resources in a vCloud Director instance, type the name of the vCloud Director instance. SQL wildcard expressions are allowed. Discovers all virtual machines managed by the vCloud Director instance.
Org Name Filter	To run the query against an organization in a vCloud Director instance, type the name of the organization. SQL wildcard expressions are allowed. Discovers all virtual machines in the organization.

Option	Description
vDC Name Filter	To run the query against a virtual datacenter in a vCloud Director instance, type the name of the virtual datacenter. SQL wildcard expressions are allowed. Discovers all virtual machines in the virtual datacenter.
vApp Name Filter	To run the query against a vApp, type the name of the vApp. SQL wildcard expressions are allowed. Discovers all virtual machines in the vApp.
VM Name Filter	To run the query to add a specific virtual machine, type the name of the machine. SQL wildcard expressions are allowed. Discovers the virtual machine.
Network Name Filter	To run the query against resources on a particular network, type the name of the network. SQL wildcard expressions are allowed. Discovers all virtual machines on the network.
IP Address Filter	To run the query to add virtual machines with a particular IP address, type the address. SQL wildcard expressions are allowed. Discovers all virtual machines with that IP address.
Include rule in post collection IP update	Select **Yes** to include the properties of this discovery rule to update the connection string information for the discovered machines when new vCloud Director data is collected. Select **No** to not update the connection string information.

8. On the Important page, select the options and click **Finish**.

Option	Description
Would you like to run this Discovery Rule now?	Select **Yes**.
License and Install Agent on Discovered Machines	If you do not use NAT mapping, select the option to install the Agent. If you use NAT mapping, you must manually install the Agent on the discovered machines.

What to do next

- Review the discovery jobs to determine if your job finished. Click **Administration** and select **Job Manager > History > Other Jobs**.
- Review the collected vCloud Director vApp virtual machine data. Click **Administration** and select **Machines Manager**. In **Available Machines** and **Licensed Machines**, select the operating system type and review the list for the added virtual machines.

- If the discovered machines are listed only in the Available Machines list and the virtual machines use NAT mapping, you must manually install the Agent appropriate for the operating system. For Windows operating systems, see "Manually Install the VCM Windows Agent" on page 84. For UNIX/Linux operating systems, see "Install the Agent on UNIX/Linux Machines" on page 114.

vCloud Director Collection Results

The vCloud Director data is collected using a collection filter with the Custom Information (Win) data type. The collected data appears in the Console. The discovered vApp virtual machines appear in Administration. After you license the virtual machines and install the Agent, you manage them based on their operating system.

The displayed data is only as current as the last time you collected data from your vCloud Director instances and from your managed machines.

Option	Description
Console	Displays collected vCloud Director instance data. Click **Console** and select **Windows tab > Operating System > Custom Information**. Select a view and select **vCloud**.
Compliance	Access compliance rules you create based on the collected vCloud Director data using the Custom Information (Win) data type. The compliance rules for the discovered virtual machines are created based on operating system.
Reports	Run a preconfigured vCloud Director report. Click **Reports** and select **Machine Group Reports > Virtual Environments > vCloud Director Managed VMs**. The report includes the vCloud Director Instance, Organization, Organization virtual datacenter, vApp Name, the VC Machine Name, and the related networking data.
Administration	Displays managed vCloud Director instances from which you are collecting data. Click **Administration** and select **Machines Manager > Licensed Machines > Licensed vSphere Systems**. Displays the discovered virtual machines with a machine name that is based on your configuration options in the discovery rule. For example, OrgName:vAppName:VirtualMachineName. Click **Administration** and select **Machines Manager**. ■ If the machines are not licensed and the Agent is not installed, the machines appear in the Available Machines data grid based on the operating system. ■ If the machines are licensed and the Agent is installed, the machines appear in the Licensed Machines data grid based on the operating system.

Configure the vSphere Client VCM Plug-In

The vSphere Client VCM Plug-In provides contextual access to VCM change, compliance, and management functions, in addition to direct access to collected vCenter, virtual machine host, and virtual machine guest data.

When using the vSphere Client VCM Plug-In, the virtual machine host name in vCenter must match the virtual machine host name in VCM.

CAUTION Anyone accessing VCM and the vSphere Client must have a unique login. Do not share vSphere Client logins between VCM users. Do not share vSphere Client logins between VCM users and non-VCM users.

Procedure

1. "Register the vSphere Client VCM Plug-In" on page 163

   The registration process configures the URL in the VMware vSphere Client to the VCM Collector and makes the **VCM Summary** and **VCM Actions** tabs available in the vSphere Client.

2. "Configuring the vSphere Client VCM Plug-In Integration Settings" on page 164

   Configure integration settings in VCM for your vSphere Client VCM Plug-In users. The settings enable users to view the VCM reports.

3. "Manage Machines from the vSphere Client" on page 165

   vSphere Client-managed machines are available in the vSphere Client VCM Plug-In when they licensed and have the VCM Agent installed. The available actions include collecting new data and running compliance, patching, and reports for the selected machines.

Register the vSphere Client VCM Plug-In

The registration process configures the URL in the VMware vSphere Client to the VCM Collector and makes the **VCM Summary** and **VCM Actions** tabs available in the vSphere Client.

The plug-in is installed automatically with VCM. To unregister a previous version of the plug-in, see "Upgrade the vSphere Client VCM Plug-In" on page 63.

IMPORTANT The account that you use to register the vSphere Client VCM Plug-In should be a local administrator on the vSphere instance. The account must connect to a machine that has a valid SSL certificate or must register an invalid certificate (for example, a development certificate) when that user logs into the vSphere Client.

Prerequsites

- Verify that you are using VMware vCenter 4 Server.
- Verify that the VMware vSphere Client is installed.
- Verify that the VMware Tools are installed on the virtual machines.

Procedure

1. On the VCM Collector, browse to `[path]\VMware\VCM\Tools\vSphere Client VCM Plugin\bin` and double-click `VCVPInstaller.exe`.
2. In the VCVP Plug-in Registration dialog box, configure these options.

Option	Description
Register	Select the option to register the URL for the plug-in. Select Unregister only if you are discontinuing the use of the plug-in on the target vSphere Client.
Server URL	Type the http or https path, where <server> is your vSphere Client server.
Administrator User Name	Type the name of a user with Administrator privileges in the vSphere Client.
Administrator Password	Type the associated password.
URL to vSphereClientVCMPlugin.xml	Type the http path, where <VCMserver> is the name or IP address for the VCM Collector. The xml file is located in `\VMware\VCM\WebConsole\L1033\VCVPAnon\Xml\vSphereClientVCMPlugin.xml`

3. Click **OK**.
4. Start VCM.
5. On the login screen, select the role that you are using to log into the vSphere Client VCM Plug-In and select the **Automatically log in using this role** check box.
6. Start the vSphere Client.
7. Select a Guest machine.

What to do next

- Confirm that you can access the **VCM Summary** and **VCM Actions** tabs.
- Configure the vSphere Client VCM Plug-In integration settings in VCM. See "Configuring the vSphere Client VCM Plug-In Integration Settings" on page 164.

Configuring the vSphere Client VCM Plug-In Integration Settings

Configure integration settings in VCM for your vSphere Client VCM Plug-In users. The settings enable users to view the VCM reports.

Prerequisites

Verify that the vSphere Client VCM Plug-In is registered. See "Register the vSphere Client VCM Plug-In" on page 163.

Procedure

1. Select **Administration > Settings > Integrated Products > VMware > vSphere Client VCM Plug-In**.
2. Select the setting you want to configure and click **Edit Settings**.
3. On the Settings Wizard page for each setting, configure the options.

Option	Description
Machine group against which the external reports will be run	Type the name of the machine group. The default value is All Machines.
Role to use for external report access	Type the name of the user role to be used to access the reports. The default value is Read-Only. Users other than Admin must have the role selected here in order to see reports in the vSphere Client.
User name to use for assessments	Type the name of the user who will be running assessments to obtain data for generating reports.

4. Click **Next**.
5. Verify your settings and click **Finish**.

What to do next

You manage machines by running compliance, patching, and reports. See "Manage Machines from the vSphere Client" on page 165.

Manage Machines from the vSphere Client

vSphere Client-managed machines are available in the vSphere Client VCM Plug-In when they licensed and have the VCM Agent installed. The available actions include collecting new data and running compliance, patching, and reports for the selected machines.

Prerequisites

- License Windows and UNIX\Linux virtual machines. See "License Windows Machines" on page 80 and "License UNIX/Linux Machines" on page 114.
- Install the Agent on the virtual machine. See "Install the VCM Windows Agent on Your Windows Machines" on page 83 and "Install the Agent on UNIX/Linux Machines" on page 114.
- Verify that the integration settings are configured. See "Configuring the vSphere Client VCM Plug-In Integration Settings" on page 164.

Procedure

1. Start the vSphere Client.
2. Click the **VCM Actions** tab.

What to do next

Click help on the **VCM Actions** tab for more information about the actions.

Troubleshooting the vSphere Client VCM Plug-In Registration

With the vSphere Client VCM Plug-In, you can view and run certain VCM actions in the vSphere Client.

You can use troubleshooting options to identify and resolve any problems.

Invalid Certificate on a vSphere Client

The vSphere Client connects to the vCenter Server using the SSL certificate and displays the datacenters, hosts, and any clusters.

Problem

When logging into a vSphere Client for the first time, if the certificate is not valid, a security warning about the SSL certificate appears.

Cause

The certificate is not valid.

Solution

1. Select the **Install this certificate and do not display any security warnings for <vCenter_Server_Instance>** option.
2. Click **Ignore**.

HTTPS/SSL Is Not Configured on the Collector

If the **VCM Summary** and **VCM Actions** tabs are not displayed, the settings are improperly configured.

Problem

In the vSphere Client, you cannot see the **VCM Summary** or **VCM Actions** tabs.

Cause

If **Use SSL** was selected during VCM installation, the https/SSL is not properly configured on the Collector.

Solution

1. Open the `.xml` file specified during the registration.
2. Edit the file to reflect the configured connection method, either http or https.

vSphere Client VCM Plug-In Is Not Enabled

If the **VCM Summary** and **VCM Actions** tabs are not displayed, the plug-in is not properly configured.

Problem

In the vSphere Client, you cannot see the **VCM Summary** or **VCM Actions** tabs.

Cause

The plug-in is not enabled in the vSphere Client.

Solution

1. In the vSphere Client, select **Plug-ins > Manage Plug-ins**.
2. In the **Installed Plug-ins** area, right-click the vCenter Configuration Manager Extension plug-in, and select **Enable**.
3. Close the Plug-in Manager.

When the tabs appear, you are ready to use the vSphere Client VCM Plug-In.

Getting Started with VCM Remote

9

The VCM Remote client is the communication and management mechanism that you use to manage mobile Windows machines as they connect to and disconnect from the network.

For Windows machines that are not continuously connected to the network, the VCM Remote client listens for network events indicating it has access to the VCM Remote-related components on the VCM Internet Information Services (IIS) server. Based on the configured settings, the Collector creates requests, such as a collection request, for the remote machine that has just come online.

VCM Remote Management Workflow

To indicate the presence of the mobile Windows machine on your network, the VCM Remote client sends an HTML POST file over HTTP to a server-side component residing on the VCM Internet Information Services (IIS) server. Based on user-defined settings, the Collector auto-licenses the remote machine, installs or upgrades the VCM Windows Agent, and determines whether it should submit a collection job for that remote machine.

The Collector batches the requests and processes them at periodic intervals. This batch processing manages the problem of having 15,000 clients come online within a short time of one another and creating 15,000 individual requests.

Configuring VCM Remote Connection Types

The VCM Remote client accommodates three connection methods, including broadband, dial-up, and LAN, for Windows machines that do not have a continuous connection to the network.

To optimize the collection of the Windows machine data, you configure different collection filters for different connection types based on general bandwidth for each connection type.

- **Broadband:** DSL and cable connections can be 156Kb to more than 1Mb.
- **Dial-up:** A dial-up connection can be 56Kb or less.
- **LAN:** A local area connection to the network equal to or greater than 1Mb. A VPN connection might be available at LAN speeds but connected over the Internet.

For each connection type, you assign a customized collection filter set. For example, when a remote machine connects using a dial-up connection, you use a collection filter set that collects only key data compared to a filter set for LAN connections that collects more data from the target machines.

Using Certificates With VCM Remote

The use of certificates with VCM Remote ensures secure communication between VCM and the VCM Remote client when they are communicating outside your internal network.

The communication between the Collector and the VCM Remote client is secured using Transport Layer Security (TLS) certificates. You can use the VCM certificate or you can use an existing Enterprise certificate.

- **VCM Certificate:** A certificate generated during the installation of VCM. The VCM certificate is located on the Collector at `[install path]\VMware\VCM\CollectorData`. You must copy the `.pem` file to each target machine.
- **Enterprise Certificate:** A certificate already in the certificate store in your environment.

Determine the certificate that you are using to validate communication, either a VCM-generated or a Enterprise certificate in certificate store. By default, the installation of a Windows VCM Agent in HTTP mode adds the Collector's Enterprise Certificate to the certificate store of the client system. The VCM Remote client can also use this certificate.

After you install the VCM Remote client, the first time the remote machine connects the Collector network, it requests a Collector certificate. If the Collector certificate is trusted by the Enterprise certificate on the client, the Collector certificate is added to the client's certificate store.

Configure and Install the VCM Remote Client

You configure the VCM Remote client server-side communication settings and then install the client on target Windows machines. After it is installed, theVCM Remote client manages the communication with VCM when the remote machine is connected to the network.

Procedure

1. "Configure the VCM Remote Settings" on page 168

   You create custom filter sets for each communication method and configure the settings to ensure efficient on-going management of the mobile Windows machines managed using the VCM Remote client.

2. "Install the VCM Remote Client" on page 171

   You install the VCM Remote client on the target Windows machines that are not continuously connected to the network.

3. "Connect VCM Remote Client Machines to the Network" on page 178

   Connect your remote machine to the VCM-managed network to begin managing the machine. The VCM Remote client notifies VCM that the remote machine is on the network and it is processed based on VCM Remote settings and requires no user interaction.

When you configure Windows machines with the VCM Remote client, the client handles the communication when the remote machine connects to the network, but the machines are managed as Windows machines. See "VCM Remote Collection Results" on page 179.

Configure the VCM Remote Settings

You create custom filter sets for each communication method and configure the settings to ensure efficient on-going management of the mobile Windows machines managed using the VCM Remote client.

Procedure

1. "Create Custom Collection Filter Sets" on page 169

   You create custom collection filter sets for Dial-up, Broadband, or LAN connections to efficiently manage mobile machines using the VCM Remote client. To optimize results, create a different filter set for each connection type.

2. "Specify Custom Filter Sets in the VCM Remote Settings" on page 170

   VCM Remote supports three connection types: broadband, dial-up, and LAN. To optimize the collection of data, you must specify the collection filter set for each connection used in your environment.

3. "Specify Agent and Host File Settings" on page 170

   To ensure the VCM Remote client efficiently installs or upgrades the Agent and manages communication, you must configure the server settings on the Collector.

Create Custom Collection Filter Sets

You create custom collection filter sets for Dial-up, Broadband, or LAN connections to efficiently manage mobile machines using the VCM Remote client. To optimize results, create a different filter set for each connection type.

With filter sets based on connection type rather than using the default filter set, you can optimize collections based on the stability and speed of the connection. For example, an all encompassing collection is difficult to complete over a dial-up connection. To optimize the collection performance, you create a dial-up filter set that is limited to a few high-importance data types and would not include the File System Uploads or Emergency Repair Disk data types.

Prerequisites

Review the purpose of the different connection types to understand what to include or exclude from your collection filter sets. See "Configuring VCM Remote Connection Types" on page 167

Procedure

1. Click **Administration**.
2. Select **Collection Filters > Filter Sets**.
3. On the Collection Filter Sets data grid, click **Add Filter Set**.
4. On the Name and Description page, type a distinctive Name and Description.

   For example, use names similar to Remote Client - Broadband, Remote Client - LAN, and Remote Client - Dial-up.

5. Select **Filter Set** and click **Next**.
6. On the Filters page, select **Machine Based Filter Set**.
7. Select the filters to include in the filter set and click **Next**.
8. On the Conflicts page, resolve any data type conflicts and click **Next**.
9. On the Important page, review the summary information and click **Finish**.

What to do next

- Repeat the procedure for all the connection types for which you configure filter sets.
- Assign the filter sets to the appropriate VCM Remote settings. See "Specify Custom Filter Sets in the VCM Remote Settings" on page 170.

Specify Custom Filter Sets in the VCM Remote Settings

VCM Remote supports three connection types: broadband, dial-up, and LAN. To optimize the collection of data, you must specify the collection filter set for each connection used in your environment.

When a mobile Windows machine connects to the network using one of three connection types and the VCM Remote client indicates the presence of the machine, VCMdetermines the connection type and uses the collection filter specified for the connection when collecting data from the target machine. This method enables mobile VCM Remote client machines to connect using any of the connection types and to collect data using a filter set optimized for the connection type.

Prerequisites

Create VCM Remote collection filter sets, one for each connection type. See "Create Custom Collection Filter Sets" on page 169.

Procedure

1. Click **Administration**.
2. Select **Settings > General Settings > VCM Remote**.
3. On the VCM Remote Settings data grid, select each setting separately and click **Edit Settings**.
   - Name of the Collection Filter Set Remote will use for Broadband connections
   - Name of the Collection Filter Set Remote will use for Dialup connections
   - Name of the Collection Filter Set Remote will use for LAN connections
4. On the Edit Settings page, select the related filter set in the drop-down list and click **Next**.
5. On the Important page, review the summary and click **Finish**.

What to do next

- Repeat the procedure for the other settings.
- Configure the Agent and host file settings. See "Specify Agent and Host File Settings" on page 170.

Specify Agent and Host File Settings

To ensure the VCM Remote client efficiently installs or upgrades the Agent and manages communication, you must configure the server settings on the Collector.

Procedure

1. Click **Administration**.
2. Select **Settings > General Settings > VCM Remote**.
3. On the VCM Remote Settings data grid, select each setting separately and click **Edit Settings**.

Option	Configuration
Should Remote automatically install an Agent to the client (if required)?	Click **Yes**. Allows VCM to install the Agent when contacted by the VCM Remote client the first time.
Should Remote automatically upgrade an Agent to the client (if required)?	Click **Yes**. Allows VCM to upgrade the Agent when contacted by the VCM Remote client.
Will IP Address of calling client be added to local host file?	Click **Yes**. Adds the IP address of the VCM Remote client to the host file to ensure that the remote client name is resolved and updated so that communication can begin.
Minutes to retain host File Entry	Type 30 or greater to specify 30 minutes or longer. Retains the IP address of the VCM Remote client in the host file for the set time to ensure that the remote client name is quickly resolved and updated during that time.

4. Configure the setting and click **Next**.
5. On the Important page, review the summary and click **Finish**.

What to do next

- Repeat precedure for the other settings.
- Install the VCM Remote client. See "Install the VCM Remote Client" on page 171.

Install the VCM Remote Client

You install the VCM Remote client on the target Windows machines that are not continuously connected to the network.

To install the VCM Remote client, use the method easiest to implement depending on your access to the target machines and the number of remote machines on which you are installing the client.

- "Install the VCM Remote Client Manually" on page 172

  The manual installation of the VCM Remote client is a wizard-based process that you use when you have direct access to the target machines. This process is a useful way to install the client if you are creating an image to install on other machines.

- "Install the VCM Remote Client Using a Command Line" on page 173

  You use the command line to install the VCM Remote client when you want to run an unattended installation using Group Policy or software provisioning.

- "Install the VCM Remote Client Using Windows Remote Commands" on page 175

  You use the Windows remote commands to deploy the VCM Remote client to multiple machines in your environment. The VCM Agent must be installed on the target machines.

Install the VCM Remote Client Manually

The manual installation of the VCM Remote client is a wizard-based process that you use when you have direct access to the target machines. This process is a useful way to install the client if you are creating an image to install on other machines.

Prerequisites

Determine the certificate that you are using to validate communication between the client and the Collector. See "Using Certificates With VCM Remote" on page 168.

Procedure

1. On the target machine, create a folder and copy the files from the Collector to the target folder.

File	Description
`CM Remote Client.msi`	Located on the Collector at `[install path]\VMware\VCM\AgentFiles`.
`CM_Enterprise_Certificate_xxx.pem`	(Optional) Located on the Collector at `[install path]\VMware\VCM\CollectorData`. Copy the file if you do not have or are not using the Enterprise certificate located in the remote machine's certificate store.

2. On the target machine, double-click the `CM Remote Client.msi` file.
3. On the VCM Remote Client Setup page, click **Next**.
4. On the Installation Folder page, accept the default installation location or click **Change** to enter a different location, and click **Next**.

5. On the VCM Remote Client Information page, configure the options and click **Next**.

Option	Description
Collector Machine Name	Name of the Windows machine on which the VCM Collector and Microsoft IIS are installed.
Path to ASP Page	Path for the IIS default VCM Remote Web site. The <virtual directory name> must match the virtual directory name as it appears in the Collector's IIS. The default value is VCMRemote.

6. On the Select Certificates page, configure the certificate option that supports your environment and click **Next**.

Option	Description
Certificate File	Use the VCM-generated `.pem` file you copied from the Collector. Browse to the location of the copied `.pem` file.
Skip Certificate Deployment	Use the existing Enterprise certificate in the client certificate store. Select the option to use the existing Enterprise certificate.

7. On the Ready to install CM Remote Client page, click **Install**.
8. Click **Finish** when the installation is completed.

What to do next

Connect the remote machine to the network to ensure that VCM completes the installation process. See "Connect VCM Remote Client Machines to the Network" on page 178

Install the VCM Remote Client Using a Command Line

You use the command line to install the VCM Remote client when you want to run an unattended installation using Group Policy or software provisioning.

Prerequisites

Determine the certificate that you are using to validate communication between the client and the Collector. See "Using Certificates With VCM Remote" on page 168.

Procedure

1. On the target machine, create a folder and copy the files from the Collector to the target folder.

File	Description
CM Remote Client.msi	Located on the Collector at [install path]\VMware\VCM\AgentFiles.
CM_Enterprise_Certificate_xxx.pem	(Optional) Located on the Collector at [install path]\VMware\VCM\CollectorData. Copy the file if you do not have or are not using the Enterprise certificate located in the remote machine's certificate store.

2. At a command prompt, edit the installation command for you environment, and run the command.

   If the names and paths contain spaces, you must use double quotation marks.

```
msiexec.exe /qn /i "[path]\cm remote client.msi" COLLECTOR="YourCollectorName"
 PATHTOASP="VCMRemote/ecmremotehttp.asp" INSTALLDIR="c:\Program Files
(x86)\VMware\VCM Remote Client” CERTIFICATE_
FILE="[path]\YourEnterpriseCertificateName.pem" /l*v "[path\]filename.log"
```

Option	Description
/qn	No error messages appear during installation.
[path]\cm remote client.msi	Path to the CM Remote Client.msi on the target machine.
COLLECTOR=YourCollectorName	Replace <YourCollectorName> with the name of your VCM Collector.
PATHTOASP=VCMRemote/ecmremotehttp.asp	Path to the IIS Default Web Site virtual directory containing ecmremotehttp.asp.
INSTALLDIR:c:\Program Files (x86)\VCM\CM Remote Client	Path where you want the VCM Remote client files installed. The directory is created by the command.
CERTIFICATE_FILE=[path]\YourEnterprise CertificateName.pem	Certificate path and name on the target machine. If you are using an existing Enterprise certificate in the client certificate store, you use SKIP_CERTIFICATE_FILE=1 instead of CERTIFICATE_FILE=[path]\YourEnterpriseCertificateName.pem. If the certificate does not exist in the store, any communication between the client and the Collector will fail.
/l*v [path\]filename.log	Error messages added to the log file in the specified path. If the path is not specified, the log file is saved in the directory from which the msiexec.exe was run. The log files are a useful troubleshooting tool.

What to do next

Connect the remote machine to the network to ensure that VCM completes the installation process. See "Connect VCM Remote Client Machines to the Network" on page 178

Install the VCM Remote Client Using Windows Remote Commands

You use the Windows remote commands to deploy the VCM Remote client to multiple machines in your environment. The VCM Agent must be installed on the target machines.

The script installs the VCM Remote client under the Windows directory rather than the Program Files directory. It is not necessary to create the install directory on the target machine before you run the script.

Prerequisites

- Verify that the Agent is installed on target machines. See "Discover, License, and Install Windows Machines" on page 77.
- Indentify the certificate you are using to validate communication between the client and the Collector. See "Using Certificates With VCM Remote" on page 168.

Procedure

1. On your Collector, copy `[install path]\Enterprise Configuration Manager\AgentFiles\CM Remote Client.msi` to `[install path]\Enterprise Configuration Manager\WebConsole\L1033\Files\Remote_Command_Files`.
2. On your Collector, copy `[install path]\Enterprise Configuration Manager\CollectorData\<YourEnterpriseCertificate>.pem` to `[install path]\Enterprise Configuration Manager\WebConsole\L1033\Files\Remote_Command_Files`.
3. In VCM, select **Console > Windows Remote Commands**.
4. On the data grid toolbar, click **Add**.
5. On the Name and Description page, type a unique name and description for the command, and click **Next**.
6. On the **Remote Command** page, configure the command.
   a. In the **Type** drop-down list, select VBScript.
   b. In **Command Text** text box, copy and paste the script and modify it as specified in the script comments.

```
Call DoWork

'Copyright 1999-2010 VMware, Inc.

'Coded by Ryan L.

'Description: Installs VCM Remote ver. 2

'Modified 4/27/2008 - Stephen S. Included Certificate file options

'Modified 7/7/2010 - VCM

Dim sCollName, sInstallDir, sVirDir, sAddRemove, sCertFile, bInstallCert

Sub DoWork()

Set WshShell = CreateObject("WScript.Shell")
```

```
sCollName = "YourCollectorName" 'Name of your VCM Collector machine in
quotes

bInstallCert = 1 'If the value is 1, the Enterprise Certificate is
installed. If the value is set to 0, the installation of the certificate is
skipped and it is assumed that the certificate is already present. The
Remote Client will NOT function until the Enterprise Certificate is
installed as specified in Step 2

sCertFile = "EnterpriseCert" 'The filename of your enterprise certificate
(.pem file) as identified in Step 2

sVirDir = "VCMRemote/EcmRemoteHttp.asp" 'Where you replace CMRemote with
the IIS Default Web Site virtual directory containing the ECMRemoteHTTP.asp
 file

sInstallDir = WshShell.ExpandEnvironmentStrings("%windir%") & "\VMware\VCM
Remote Client" 'The installation directory on the TARGET machine

sAddRemove = 1 'Whether or not VCM remote should appear in the Add/Remove
programs List, should be 0 = hide, 1 = show

sMSIPackageName = "CM Remote Client.msi" 'Name of the MSI package that
installs VCM Remote Agent


CheckVars


If sAddRemove = 0 Then

AppToRun = "msiexec.exe /qn /i " & Chr(34) &
EcmAgtContext.JobDownloadDirectory & "\" & sMSIPackageName & Chr(34) & "
ALLUSERS=1 COLLECTOR=" & Chr(34) & sCollName & Chr(34) & " PATHTOASP=" &
Chr(34) & sVirDir & Chr(34) & " ARPSYSTEMCOMPONENT=" & sAddRemove & "
INSTALLDIR=" & Chr(34) & sInstallDir & Chr(34)

Else

AppToRun = "msiexec.exe /qn /i " & Chr(34) &
EcmAgtContext.JobDownloadDirectory & "\" & sMSIPackageName & Chr(34) & "
ALLUSERS=1 COLLECTOR=" & Chr(34) & sCollName & Chr(34) & " PATHTOASP=" &
Chr(34) & sVirDir & Chr(34) & " INSTALLDIR=" & Chr(34) & sInstallDir &
Chr(34)

End If

If bInstallCert = 1 Then

AppToRun = AppToRun & " CERTIFICATE_FILE=" & Chr(34) &
EcmAgtContext.JobDownloadDirectory & "\" & sCertFile & Chr(34)

Else

AppToRun = AppToRun & "SKIP_CERTIFICATE_FILE=1"

End If

EcmScriptRuntime.CmdExecute Chr(34) & AppToRun & Chr(34), 10000
```

```
End Sub

Sub CheckVars()
If sCollName = "" Then
WScript.Quit
Else
sCollName = Trim(sCollName)
End If

If sVirDir = "" Then
sVirDir = "vcmremote/ecmremotehttp.asp"
Else
sVirDir = Trim(sVirDir)
End If

If sInstallDir = "" Then
sInstallDir = "c:\vcm remote client"
Else
sInstallDir = Trim(sInstallDir)
End If

If sAddRemove <> 0 And sAddRemove <> 1 Then
sAddRemove = 1 'Set whether or not VCM Remote appears in the Add/Remove
programs list. 1=display, 0=do not display
End If

If sAddRemove = "" Then
sAddRemove = 1
End If

If IsNumeric(sAddRemove) = False Then
sAddRemove = 1
End If

sAddRemove = Trim(sAddRemove)
```

```
End Sub
```

c. Select the **Certain file(s) are required to be on the target machine for this remote command** check box.

d. Click **Next**.

7. On the Files page, move the `CM Remote Client.msi` file and the `.pem` file to the list on the right, and click **Next**.

   These are the files you added to the `[install path]\Enterprise Configuration Manager\WebConsole\L1033\Files\Remote_Command_Files` directory.

8. On the Important page, review and summary and click **Finish**.

   VCM saves and adds the command to **Windows Remote Commands** list.

9. In the Windows Remote Commands data grid, select your VCM Remote installation remote command and click **Run**.

10. On the Machines page, select the Windows machines on which you are installing VCM Remote.

11. On the Schedule page, select when to run the installation and click **Next**.

    If you are running the installation command on many Windows machines at one time, schedule the installation for non-peak network hours.

12. On the Important page, review the summary to verify the number of target machines and click **Finish**.

What to do next

- Verify that the installation is finished. To view the status of the Install CM Remote Client job, click **Administration** and select **Job Manager > History > Instant Collections**.
- Connect the remote machine to the network to ensure that VCM completes the installation process. See "Connect VCM Remote Client Machines to the Network" on page 178

Connect VCM Remote Client Machines to the Network

Connect your remote machine to the VCM-managed network to begin managing the machine. The VCM Remote client notifies VCM that the remote machine is on the network and it is processed based on VCM Remote settings and requires no user interaction.

Prerequisites

- Configure the VCM Remote server settings. See "Configure the VCM Remote Settings" on page 168.
- Install the VCM Remote client on target machines. See "Install the VCM Remote Client" on page 171.

Procedure

1. Connect the remote machines to the VCM managed network.

   VCM Remote client sends an POST request to the VCM IIS server indicating its presence on the network. The Collector processes the request, auto-licenses the remote machine, installs or upgrades the VCM Windows Agent, and determines whether it should submit a collection job for that remote machine.

What to do next

Review the collected data. See "VCM Remote Collection Results" on page 179.

VCM Remote Collection Results

The VCM Remote client-specific data is limited to administrative details. All other data collected from the remote machine appears in VCM as Windows machine data. See "Windows Collection Results" on page 91.

The displayed data is only as current as the last time you collected from the remote machines.

Option	Description
Administration	View administrative details about the VCM Remote client. ■ To view the installed Remote client version, click **Administration** and select **Machines Manager > Licensed Machines > Licensed Windows Machines**. The Remote Client Version appears in the data grid. ■ To view the status of remote collection jobs, click **Administration** and select **Job Manager > History > VCM Remote**.

Getting Started with VCM Patching 10

VCM Patching for Windows and UNIX/Linux Machines

VCM Patching is the VCM patch assessment, deployment, and verification capability, which ensures continuous enterprise security through proactive compliance of the IT infrastructure. VCM Patching ensures that your machines have the latest security patches and other software downloads. You can evaluate each licensed machine in your network for the current Microsoft Security Bulletins or supported UNIX and Linux Vendor Bulletins and deploy the recommended patches to each machine.

Before you patch Windows 2008 servers and Windows 7 machines, make sure the Windows Update service is running (set to something other than Disabled) or the patch deployment will fail.

IMPORTANT For VCM Patching to correctly assess Windows systems, you must have a current collection of File System, Hotfixes, Registry and Services data. VCM Patching uses the File System, Registry and Services data to determine which applications that might require patches are installed and running, and uses the Hotfixes data to determine which patches are already installed on which machines. VCM Patching for UNIX and Linux machines collects the data when you perform an assessment.

VCM Patching for Windows Machines

VCM Patching for Windows provides several features that help you deploy patches to remediate Windows machines.

- **Bulletins**: Lists Microsoft bulletins available to VCM Patching. You can view these bulletins by bulletin and by affected product.
- **Assessment Templates**: Contains one or more bulletins. When you run an assessment, the machines that require the patches described by each bulletin appear. You can select bulletins or product names to create templates.
- **Imported Templates**: A user-defined template that associates machines with patches for the deployment of those patches to selected machines. Imported templates are available for Windows machines.
- **VCM Patching Administration**: Configures E-mail notifications, proxy server and logon information, machine group mapping for custom patching, and administration tasks for Windows and UNIX machines. You can select the machines for VCM Patching to manage, add and update your VCM Patching license, and view the status of jobs that are running, scheduled, and completed.

VCM Patching for UNIX and Linux Machines

VCM Patching for UNIX and Linux provides several features to deploy patches to remediate UNIX and Linux machines.

- **Bulletins**: Lists of vendor bulletins available to VCM Patching.
- **Assessment Templates**: Contains one or more bulletins that dynamically display the machines that require the patches described by each bulletin. You can select bulletins or product names to create templates.
- **Imported Templates**: A user-defined template that associates machines with patches for deployment of those patches to selected machines. Imported templates are available for UNIX and Linux machines.
- **Assessment Results**: Displays the results of your assessment for all bulletins or for specific bulletins.
- **VCM Patching Administration**: Configures E-mail notifications, proxy server and logon information, machine group mapping for custom patching, and administration tasks for Windows and UNIX machines. You can select the machines for VCM Patching to manage, add and update your VCM Patching license, and view the status of jobs that are running, scheduled, and completed.

Minimum System Requirements

VCM Patching must be installed on the same machine as VCM because it requires the VCM database. VCM data must be collected for VCM Patching to have the required information. You should collect all data types, but as a minimum you must collect Hotfixes, File System, Registry and Services data.

UNIX and Linux Patch Assessment and Deployment

VCM Patching includes UNIX and Linux patch assessment and deployment, which you use to determine the patch status of UNIX and Linux machines.

NOTE Assessments of UNIX and Linux machines operate differently from Windows assessments. UNIX and Linux assessments require you to collect new data. Windows assessments are performed against previously collected data.

Before you use VCM Patching to install patches on UNIX and Linux machines, you must collect patch assessment data from those machines.

VCM Patching for UNIX and Linux involves the process illustrated in the following steps and diagram.

1. You check for patch bulletin updates from the download site.

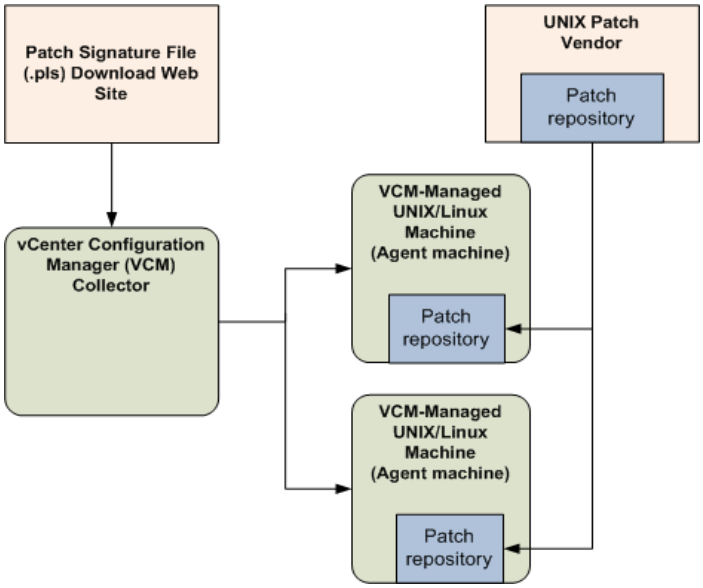
   New `PLS` files are downloaded to the VCM Collector.

2. You use VCM to collect and assess machine data from managed machines.

   During the collection, the `PLS` files are sent to the managed UNIX/Linux machines.

3. You use VCM to explore the assessment results and determine the patches to deploy.
4. You acquire and store the patches using FTP, HTTP, or any other method.
5. You use the VCM Deploy wizard to install the UNIX patches on the managed machines.

Figure 10–1. UNIX and Linux Patch Assessment and Deployment Process



To verify that VCM supports your UNIX and Linux machines for patch deployment, see the *VCM Hardware and Software Requirements Guide*.

VCM provides patch assessment content in a new format for several Red Hat and SUSE versions. See "New UNIX Patch Assessment Content" on page 183. For the operating system versions supported, see the *VCM Hardware and Software Requirements Guide*.

New UNIX Patch Assessment Content

VCM provides patch assessment content in a new format for several Red Hat and SUSE versions. For the operating system versions supported, see the *VCM Hardware and Software Requirements Guide*. All other UNIX and Linux versions use the standard content architecture.

When the VCM 5.4.1 or later Agent is installed on these machines, VCM supports patch assessments using the new content architecture.

With the new patch assessment content, VCM updates the information required to assess the patch status of your VCM managed Red Hat and SUSE machines. Results for the new and standard patch assessment content formats appear together in a single view in VCM. Use these results to analyze the patch status of all versions of your Red Hat and SUSE machines regardless of the VCM Agent version installed on them.

Patch deployment to all Red Hat and SUSE managed machines that include a combination of VCM pre-5.4.1 and 5.4.1 or later Agents installed uses a single action. In earlier versions of supported Red Hat and SUSE operating systems that have a pre-5.4.1 Agent installed, the pre-5.4.1 content is enabled automatically for patch assessments.

Patch Bulletin Name Changes

In the assessment results, patch bulletins appear with titles that differ from the standard content.

Managed Machine	New Bulletin Title	Standard Bulletin Title
Red Hat 4, 5, and 6	`RHBA-2005:356-06`	`RH 2005:356-06 (RHBA)`
SUSE SLES 10.0–10.3, 11.0–11.1	`Novell SUSE 2010-09-16 x86_64: Security update for bzip2`	`Novell Linux 2010-09-16 x86_64: Security update for bzip2`

The .pls files use new names. Red Hat file names include Red Hat instead of RH, and SUSE file names include Novell SUSE instead of Novell Linux.

Patch Assessment Content Private Repository

The new patch assessment content architecture uses a private YUM repository to contain the VCM patch assessment content for Red Hat and SUSE machines. This content supports several Red Hat and SUSE versions that have the VCM 5.4.1 or later Agent installed.

The VCM 5.4.1 installation process installs the repository in the CMAgent directory on the Collector machine. During a UNIX patch assessment of the Red Hat or SUSE machines, VCM copies the repository from the Collector to the managed machines. VCM Patching accesses the content in this repository to perform the patch assessments on those machines.

Installed Patch Assessment Files

A patch assessment of the Red Hat and SUSE machines creates several files in the /tmp directory. These files include yrl.txt, yli.txt, and yls.txt. At the start of each patch assessment process, VCM removes these files and recreates them during the patch assessment.

When you perform a patch assessment of the Red Hat or SUSE machines, the VCM 5.4.1 Agent installation process uses a script named mcescan to access the local private repository on the managed machine. The mcescan script resides in the /usr/bin/ directory on the managed machine.

Patch Assessment Content Download Settings

The administration settings in VCM enable the patch assessment content download to the Collector. During a patch assessment, the Collector copies the patch assessment content to your Red Hat and SUSE machines based on the VCM Linux Agent installed on those machines.

- Managed machines that have the VCM 5.4.1 or later Agent installed use the new content architecture.
- Managed machines that have the VCM 5.4.0 or earlier Agent installed use the standard content architecture.

Getting Started with VCM Patching

Use VCM Patching to assess the state of managed Windows, UNIX, and Linux machines, and deploy patches to those machines.

"Getting Started with VCM Patching for Windows Machines" on page 184

"Getting Started with VCM Patching for UNIX and Linux Machines" on page 191

For information about other VCM Patching functionality, such as Windows patch staging or to create filters for UNIX patch assessment results, see the online help.

Getting Started with VCM Patching for Windows Machines

Use VCM Patching to determine the patch status of Windows machines and deploy patches to those machines.

Prerequisites

To deploy patches to Windows or UNIX/Linux machines, UNIX machines in single-user mode, or AIX machines, you must understand the actions in the deployment and perform several prerequisites. See "vCenter Software Content Repository Tool" on page 190.

Procedure

1. "Check for Updates to Bulletins" on page 185

   Use VCM Patching to check the Web for updates to patch bulletins, which you can use in assessments of machines to enforce compliance.

2. "Collect Data from Windows Machines by Using the VCM Patching Filter Sets" on page 185

   Collect data from Windows machines to obtain the current patch status. VCM Patching requires you to collect current information about the File System, Hotfixes, Registry, and Services Windows data types.

3. "Assess Windows Machines" on page 186

   Use an assessment template to assess the patching status of Windows machines.

4. "Review VCM Patching Windows Assessment Results" on page 187

   View the assessed Windows machines. The Assessment Results data grid displays the Windows machines that were assessed, the patch status for each machine, and details about the patches.

5. "Deploy Patches to Windows Machines" on page 190

   Deploy patches to Windows machines that are managed by VCM Patching.

6. "Collect Data from Windows Machines by Using the VCM Patching Filter Sets" on page 185

   Collect data again from Windows machines to obtain the updated patch status.

7. "Assess Windows Machines" on page 186

   Run another assessment to assess the updated patch status of Windows machines.

Check for Updates to Bulletins

Use VCM Patching to check the Web for updates to patch bulletins, which you can use in assessments of machines to enforce compliance.

Procedure

1. Click **Patching**.
2. Select **Windows > Bulletins**.
3. To obtain a comprehensive view of all released bulletins, click **By Bulletin**.
4. To find a bulletin for an installed software product, click **By Affected Product**.
5. Select **Check for Update**.
6. If updates exist, download the updates.

   VCM displays a dialog box communicating the status of your request. Follow the prompts to update your bulletins, force an update to the bulletins, or cancel the request.

7. Click **Finish** to submit the download job to the pending job queue.

   When the job is finished running, the content is available in VCM.

Collect Data from Windows Machines by Using the VCM Patching Filter Sets

Collect data from Windows machines to obtain the current patch status. VCM Patching requires you to collect current information about the File System, Hotfixes, Registry, and Services Windows data types.

Procedure

1. On the toolbar, click **Collect**.
2. Select the Windows machines from which to collect data.
3. Select **Select a Collection Filter Set to apply to these machines** and click **Next**.
4. Select the **Patching - Windows Security Bulletins** filter set and click **Next**.

   The Patching - Windows Security Bulletins filter set for Windows machines gathers information for all bulletins. Bulletin filter sets are available by month, and you can select any of the monthly filter sets to filter the bulletins released in that month.
5. If no conflicts appear, click **Finish** to begin the collection.

   If problems occur while collecting data from Windows machines using the VCM Patching Filter Sets while using the default Network Authority Account, either give the account access to the Windows servers or use a separate Network Authority Account for these machines. See Default Network Authority Account for more information.

Assess Windows Machines

Use an assessment template to assess the patching status of Windows machines.

Because the assessment is run only against data in the database, you must collect machine patching data before and after you run an assessment. When run, the template checks data collected from machines to confirm whether the patches referenced by the bulletins must be installed on those machines. For example, a template might contain all bulletins related to Internet Explorer 7 to ensure that all of the instances installed have the latest security fixes.

The assessment checks all of the VCM-managed machines in the active machine group. A patch deployment applies only to the machines in the machine group that are managed by VCM Patching.

You can create an assessment template in several ways: based on bulletins, based on affected software products, or by importing a text file that lists machines that require a particular patch or that lists machine and patch pairs. The following procedure generates an assessment template based on bulletins.

Procedure

1. Review the collected patching data and determine which machines must be patched.
2. Click **Patching**.
3. Select **Windows > Bulletins > By Bulletin**.
4. Select a bulletin.
5. Click **Details** and read the technical details about the bulletin, including the affected products and vendor recommendations.
6. Read the Deployment Summary to identify any issues that might interfere with the distribution of the bulletin.
7. Click **On the Web** to link to vendor information about the bulletin.
8. Review all of the bulletins to include in the assessment template.
9. To create a template that includes all of the bulletins for patches to deploy, select all of the relevant bulletins and click **Create Template**.
10. Verify that the bulletins are selected and click **Finish** to create the template.

11. On the VCM toolbar, verify that the correct Machine Group is selected.
12. Click **Patching** and select **Windows > Assessment Templates**.
13. Select the template to run and click **Assess**.
14. When the assessment completes, indicated by the Assessment Results pop-up dialog box, click the **Refresh** button on the toolbar and view the assessment results in the data grid.

Review VCM Patching Windows Assessment Results

View the assessed Windows machines. The Assessment Results data grid displays the Windows machines that were assessed, the patch status for each machine, and details about the patches.

Prerequisites

Run an assessment template.

Procedure

1. Click **Patching**.
2. Select **Windows > Assessment Templates**
3. Select the template and view the results in the data grid.
4. View the Patch Status column to determine the state of each machine for the patches listed.
5. If the assessment results provide multiple pages of data, click the **Patch Status** column heading and drag it up to **Column Grouping**.
6. In the Column Grouping view, expand the **Not Patched** status to view all of the machines that are not patched.
7. To display the graphical representation of the patch assessment status, select **Enable/Disable Summary** in the template data grid view to enable the Summary view, and click the template node again.

   The Summary view displays a graph of the patch status for the machines that were assessed and the patch status by asset classification and bulletin severity rating. The Not Patched column displays machines that require a patch or a reboot for a patch that was applied.

   From the Summary view you can drill down to the affected machines.

Prerequisites for Patch Deployment

To deploy patches to Windows or UNIX/Linux machines, UNIX machines in single-user mode, or AIX machines, you must understand the actions in the deployment and perform several prerequisites.

Assessments of UNIX and Linux machines are run against the patches known by VMware at the time the assessment is performed.

VCM saves UNIX and Linux patching change actions in the VCM change log. Click **Console** and select **Change Management > VCM or Non VCM Initiated Change > By Data Type > Patch Assessment**. These change actions are available to Compliance and Reports.

IMPORTANT If a failure occurs at any point in the patch deployment job, the System Administrator must check the status of the system, resolve any issues, and then reassess the machines.

VCM Patching Actions

- **Agent Install:** VCM Patching installs the Agent component to a machine the first time a patch is deployed to that machine.
- **Agents using HTTP:** If VCM Patching detects that the target machine has an VCM Agent using HTTP, VCM Patching will route the deployment through VCM as a remote command job.

Prerequisites

- **Test Patches:** Test all patches before you deploy them.
- **Back up critical systems:** Some patches might adversely affect target systems. Before you deploy selected patches, you must understand their potential impact and create backups of critical systems.
- **Set Administrator Privileges:** If users without Administrator privileges will use VCM Patching to deploy patches, you must modify the File-level permissions of the `\\collector_name\cmfiles$\SUM Downloads` share. This default share is shared to Everyone with Full Control, but the file permissions are more limited and the Everyone group only has read permission on the directory. Make sure that the user, or a group to which the user belongs, has write permission in the download directory.
- **Set Timing for Multiple Patch Jobs:** When one or more patches are deployed, a job is created for each machine in Patching > VCM Patching Administration > Windows or UNIX > Job Manager > Scheduled . If a reboot is required, two jobs are created for each machine, each with the same start time. If you have many machines, or if you selected to download the patches at run time, jobs might exceed the defined window before they time out. If jobs time out, you can:
  - Increase the setting, "How long before a request will be considered stale (minutes)", in Administration > Settings > General Settings > Collector.
  - Increase the setting, "Maximum Concurrent Agent Installs", in Patching > VCM Patching Administration > Settings and Options > Deployment > Collector Option.
  - Reschedule jobs in Patching > VCM Patching Administration > Job Manager > Scheduled.

Acquire the UNIX Patches

After you review the assessment results and determine which patches to deploy, use FTP, HTTP, or another available method to acquire the UNIX patches from the appropriate vendor.

Store the UNIX Patches

Store the UNIX patches in a location that is available locally to the VCM-managed machine, such as an NFS mount or a local hard drive. If you store the patches on an NFS mount, you must define the path in **Patching > VCM Patching Administration > Machine Group Mapping**. You can use VCM remote commands or another available method to place the patches on the VCM-managed machines.

Patch Repository Management

You must manage your own patch repository. A temporary expansion of the patches occurs in the `/tmp` directory. For single-user mode, patches are extracted to `/var/tmp`. If you do not use Machine Group Mapping to define an alternate location for the patches, the default location of `/tmp` is used.

Machine Group Mapping

When you define an alternate patch location for a particular machine group, you must select that machine group in VCM before you deploy the patches. If you do not select this machine group, VCM Patching will not acknowledge the alternate patch location and the patches will not be deployed. The alternate patch location is defined in **Patching > VCM Patching Administration > Machine Group Mapping > Local Patch Path**.

Default Location for UNIX/Linux Patches

If you do not define an alternate location for the patches using Machine Group Mapping, the default location of `/tmp` is used. A temporary expansion of the patches occurs in the `/tmp` directory.

Location for UNIX/Linux Patches

When patching UNIX/Linux machines, you must first copy the patches to a shared location, and then specify the local patch path location. Click **Patching** and select **VCM Patching Administration > Machine Group Mapping**.

Prerequisites to Patch in Single-user Mode on UNIX machines

If you will deploy patches in single-user mode on UNIX machines, you must perform several actions.

1. Store or extract the patches in a local location other than `/tmp` that will be accessible in single user-mode.
2. If you did not manually extract the files in step 1, ensure enough disk space exists to extract the patches in `/var/tmp`.
3. Set the machine group mapping to the patch path location where you have stored the patches.
4. To successfully deploy UNIX patches in single-user mode, the `at` daemon must be running on the machines where patches are being deployed.

If you will deploy patches without changing the run level, you must perform several actions.

1. Store or extract the patches in a local location (not `/tmp` on Solaris as this directory will be cleaned out upon reboots that may be initiated by the patches).
2. If you did not manually extract the files in step 1, ensure enough disk space exists to extract the patches in `/tmp` (or `/var/tmp` on Solaris).
3. Set the machine group mapping to the patch path location where you have stored the patches.
4. To successfully deploy UNIX patches where a reboot is required or requested, the `at` daemon must be running on the machines where patches are being deployed.

You must set the Machine Group mapping for VCM to the location of the patches during deployment. Setting the machine group mapping is especially important when patching in single-user mode because `/tmp` is not always available, and therefore cannot be relied upon for patching with VCM.

Machine Group mappings are not inherited. For example, if under the machine group called UNIX Machines, you create a machine group called Solaris, the machine group mapping that exists for UNIX Machines will not be applied to the Solaris machine group.

You can change the default machine group mapping for single-user mode by contacting VMware Technical Support.

Prerequisites to Patch AIX machines

Deploying some patches might fail on AIX machines if the patch prerequisites cannot be resolved by VCM using the downloaded patch bulletin content. This problem can arise with an AIX patch whose status is "StatusNotPatched", and where the Bulletin Detail indicates a patch dependency on another set of patches whose dependencies cannot be met.

Although dependencies may or may not appear the Bulletin Detail, one or more currently irresolvable patch dependencies may actually exist. The missing patch prerequisites can occur when some patch versions do not become applicable until after other patches are installed. In particular, Maintenance Level (ML) or Technology Level (TL) packages and their corresponding bulletins that are intended to upgrade between levels may not show as applicable until the ML/TL upgrade has been met or exceeded. For example, if you are applying a patch that depends on an intermediate ML that has not yet been applied, deploying the patch will fail since the prerequisite patch dependency has not been met.

To resolve the patch interdependencies on AIX machines, you must determine the patch strategy used for the filesets/APARS/MLs/TLs that are being updated.

Default Location for UNIX/Linux Patches

If you do not define an alternate location for the patches using Machine Group Mapping, the default location of `/tmp` is used. A temporary expansion of the patches occurs in the `/tmp` directory.

vCenter Software Content Repository Tool

To help you obtain UNIX patches for deployment, a deployment tool is available from VMware Technical Support. For more information, contact VMware Technical Support.

Deploy Patches to Windows Machines

Deploy patches to Windows machines that are managed by VCM Patching. These machines appear in **Patching > VCM Patching Administration > Windows > Machines Manager > Licensed Machines**.

Prerequisites

- Follow the guidelines in "vCenter Software Content Repository Tool" on page 190 before you deploy a patch.
- Make sure the Windows Update service is running (set to something other than Disabled) before you patch Windows 2008 servers and Windows 7 machines, or the patch deployment will fail.

Procedure

1. Click **Patching**.
2. Select **Windows > Assessment Templates** and select the template used for the assessment.
3. Make sure the data grid view is visible so that you can view the machines and bulletins.
4. Locate the rows that display the StatusNotPatched status.

   To easily identify the machines that must be patched, group the Patch Status column.
5. Highlight the row containing the machine to be patched and select **Deploy**.

   If you have VCM Service Desk Integration licensed, the Service Desk Connector dialog box appears prior to the VCM Patching Deploy wizard.

   If you licensed and activated VCM Service Desk Integration, VCM Orchestrator must approve the deployment job before it can run.
6. (Optional) Although the Deploy wizard automatically selects the machine and the patch to be deployed, you can select additional machine and patch combinations to include.

7. Select the machines and patches to deploy and click **Next**.

   The Deploy wizard attempts to detect the patch by first checking the Collector, and if found, uses the downloaded patch. If the patches are not found on the Collector, the Deploy wizard attempts to locate the patch on the Internet.

   If the patch is found on the Internet, you can choose to download the patch immediately or at run time.

   If access to the Internet is denied, you must obtain the patches manually and store them in `\\collector_name\cmfiles$\SUM Downloads` on the Collector.

8. Click **Next**.
9. If you selected multiple patches to deploy, confirm the order to deploy the patches, or reorder them, and click **Next**.
10. On the Switches page, do not select any switches for the installation, and click **Next**.
11. On the Patch Staging and Deployment Schedule page, select to copy the patches to the VCM Patching-machine during deployment.
12. Select to run the deployment immediately or schedule it to run later, and click **Next**.
13. Click **Next** to either schedule the deploy job or to instruct VCM Patching to execute the job immediately.
14. On the Reboot Options page, select to not reboot the machine and click **Next**.
15. On the confirmation page, click **Finish** to deploy the patch.

    When the deployment completes, VCM Patching automatically runs a delta collection of the VCM Patching Security Bulletins filter set to update the assessment information.

16. To view the status of the deployment job, select **Patching > VCM Patching Administration > Windows > Job Manager > Running** .
17. If you scheduled the job to run later, to view the status of the scheduled deployment, select **Patching > VCM Patching Administration > Windows > Job Manager > Scheduled > Deployments**.
18. In the assessment template data grid view, run another assessment and confirm that the machines you patched are marked as Patched in the assessment results.

    If a machine is in a pending reboot state, the patch status for the machine is Not Patched.

IMPORTANT If a failure occurs at any point in the patch deployment job, the System Administrator must check the status of the system, resolve any issues, and then reassess the machines.

For more information about scheduled patch deployments for Windows machines, see the online help.

Getting Started with VCM Patching for UNIX and Linux Machines

When licensed, you can use VCM Patching for UNIX/Linux to determine the patch status of UNIX and Linux machines and deploy patches to those machines.

NOTE Assessments of UNIX and Linux machines operate differently from Windows assessments. UNIX and Linux assessments require you to collect new data. Windows assessments are performed against previously collected data.

VCM saves UNIX and Linux patching change actions in the VCM change log. Click **Console** and select **Change Management > VCM or Non VCM Initiated Change > By Data Type > Patch Assessment**. These change actions are available to Compliance and Reports.

Prerequisites

- Collect patch assessment data from UNIX and Linux machines.
- Verify that VCM Patching for UNIX/Linux is licensed on the UNIX or Linux machine.
- Verify that your UNIX and Linux machines and operating systems are supported for patch deployment. See the *VCM Hardware and Software Requirements Guide*.

Procedure

1. "Check for Updates to Bulletins" on page 192

   Check for updates to VCM Patching bulletins before you assess the patching state of UNIX and Linux machines.

2. "Collect Patch Assessment Data from UNIX and Linux Machines" on page 192

   Collect UNIX and Linux patch assessment data using bulletins, an assessment template, or the Collect wizard.

3. "Explore Assessment Results and Acquire and Store the Patches" on page 194

   View the assessed UNIX and Linux machines. The Assessment Results data grid displays the UNIX and Linux machines that were assessed, the patch status for each machine, and details about the patches.

4. "Deploy Patches to UNIX/Linux Machines" on page 196

   Install the patches on UNIX and Linux machines that are managed by VCM Patching.

Check for Updates to Bulletins

Check for updates to VCM Patching bulletins before you assess the patching state of UNIX and Linux machines.

Prerequisites

Place patch bulletin files on the local machine to load the bulletin updates from a local file.

Procedure

1. Click **Patching**.
2. Select **UNIX/Linux Platform > Bulletins > By Bulletin**.
3. Click **Check for Update**.

   You can check for updates on the Internet or load the updates from patch bulletin files on the local machine.

4. Select **Check for Updates via the Internet** and click **Next**.

   If VCM Patching finds updates, they are downloaded to the local machine.

Collect Patch Assessment Data from UNIX and Linux Machines

Collect UNIX and Linux patch assessment data using bulletins, an assessment template, or the Collect wizard.

- **Bulletins:** Collect patching data using the Patch Assessment collection filter. Because UNIX and Linux assessments are VCM collections, you can schedule these assessments.
- **Assessment template:** Collect patching data using a template that filters the patch assessment results.
- **Collect wizard:** Collect patching data using the Patch Assessment Data Class filter.

NOTE Assessments of UNIX and Linux machines operate differently from Windows assessments. UNIX and Linux assessments require you to collect new data. Windows assessments are performed against previously collected data.

Assessments of UNIX and Linux machines are run against the patches known by VMware at the time the assessment is performed.

Patch assessments of UNIX and Linux machines are based on the OS version and machine architecture. When you collect assessment data using templates, you must match the bulletins, either 32-bit or 64-bit, to the machine architecture.

For a patch assessment that did not return any results, see the troubleshooting section.

If machine data has not been collected, the assessment results might not appear and the machine will not be available for deployment. If this situation occurs, a patch-machine mismatch status results. You can display or hide the patch-machine mismatch status. Click **VCM Patching** and select **VCM Patching Administration > UNIX > Settings > Bulletin and Update**.

Prerequisites

- Confirm that assessments finished successfully.
- Verify that the patch signature files (`.pls` files) exist on the Collector.

  The `.pls` files determine whether required patches are installed on the machine. By default, VCM Patching downloads the `.pls` files automatically every 4 hours.

  Patch files appear in **Console > UNIX > Security > Patches > Assessment or Console > Change Management > Non VCM Initiated > By Machine**. During an assessment of the machines using the Patch Assessment Data Class, the `.pls` files are sent from the Collector to the machine. A delay might occur during this process.
- Verify that the VCM Agent is installed on the UNIX or Linux machine.
- Verify that the UNIX or Linux machine is licensed for VCM Patching.
- Verify that you already have pre-configured filters if you choose **Filters** in the following procedure. See "Create UNIX and Linux Patch Assessment Filters" on page 194.

The following procedure runs the assessment using patch bulletins.

Procedure

1. On the toolbar, select the **All UNIX Machines** machine group.
2. Click **Patching**
3. Select **UNIX/Linux Platform > Bulletins > By Bulletin**.
4. Select **Assess**.
5. In the UNIX Patch Assessment wizard, select **Default Filter** or **Filters**.

   If you selected **Filters**, you must select a specific filter.
6. Click **Next** and **Finish** to begin the assessment on all machines in the selected machine group.

7. On the toolbar, click **Jobs** and view the progress of the collection.

   The assessment on UNIX and Linux machines uses the Patch Assessment collection filter to perform a collection of all machines in the current machine group, and the results are reported in the Assessment Results node.

8. Select **UNIX/Linux Platform > Assessment Results > All Bulletins** and view the results.

Create UNIX and Linux Patch Assessment Filters

Patch assessment filters identify patch bulletins that meet user-defined filtering criteria. These filters limit the bulletins to use in the assessments, which improves the efficiency of the assessment.

Procedure

1. Click **Administration**.
2. Select **Collection Filters > Filters**.
3. In the Collection Filters data grid, select **Add Filter**.
4. On the Name and Description page, name the filter and click **Next**.
5. On the Data Type page, select **UNIX/Linux**.
6. Select **Patch Assessment** and click **Next**.
7. On the **UNIX Patch Assessment Filters** page, to create a subset of the available bulletins, select **Include Bulletin(s) that match this criteria**.
8. Define the filter criteria using the available settings.

   For example, you can create a filter where **Platform = Red Hat** and **Severity = Critical**.

9. Click **Next** and **Finish** to create the filter.
10. In the Collection Filters data grid, scroll or page to the Patch Assessment in the Data Type column and locate the new filter in the Name column.

What to do next

Use the new filter when you run an assessment.

Explore Assessment Results and Acquire and Store the Patches

View the assessed UNIX and Linux machines. The Assessment Results data grid displays the UNIX and Linux machines that were assessed, the patch status for each machine, and details about the patches.

Procedure

1. Click **Patching**.
2. Select **UNIX/Linux Platform > Assessment Results > All Bulletins** to display the patch status of all of the machines that were assessed.
3. To display the assessment results for a single bulletin, select **By Specific Bulletin** and select a bulletin in the center pane.
4. Review the patch status for each machine.

Icon	Status	Description
	Patched	The patch is applied to the machine.

Icon	Status	Description
	Patch-Machine Mismatch	The patch OS version or hardware architecture does not match the machine.
	Patch Not Needed	The machine is up-to-date or the intended software product is not installed on the machine.
	Not Patched	The patch is not applied to the machine.
	Error Occurred	An unexpected condition occurred during the assessment of the machine. You can determine additional information about the root cause of the exception by running the Debug Event Viewer at `C:\Program Files (x86)\VMware\VCM\Tools\ecmDebugEventViewer.exe`.
	Signature Not Found	The `.pls` patch file does not exist on the machine and the patch status cannot be determined.
	Incorrect MD5	The MD5 Hash generated from the patch signature (`.pls`) file, which contains the content and signature, does not match the expected value on the UNIX or Linux Agent. Be aware that MD5 is NOT validated against the vendor MD5 hash data.
	Patch Status Unknown	The patch status of the machine cannot be determined.

If machine data has not been collected, the assessment results might not appear and the machine will not be available for deployment. If this situation occurs, a patch-machine mismatch status results. You can display or hide the patch-machine mismatch status. Click **VCM Patching** and select **VCM Patching Administration > UNIX > Settings > Bulletin and Update**.

Acquire the UNIX Patches

After you review the assessment results and determine which patches to deploy, use FTP, HTTP, or another available method to acquire the UNIX patches from the appropriate vendor.

Store the UNIX Patches

Store the UNIX patches in a location that is available locally to the VCM-managed machine, such as an NFS mount or a local hard drive. If you store the patches on an NFS mount, you must define the path in **Patching > VCM Patching Administration > Machine Group Mapping**. You can use VCM remote commands or another available method to place the patches on the VCM-managed machines.

Patch Repository Management

You must manage your own patch repository. A temporary expansion of the patches occurs in the `/tmp` directory. For single-user mode, patches are extracted to `/var/tmp`. If you do not use Machine Group Mapping to define an alternate location for the patches, the default location of `/tmp` is used.

Machine Group Mapping

When you define an alternate patch location for a particular machine group, you must select that machine group in VCM before you deploy the patches. If you do not select this machine group, VCM Patching will not acknowledge the alternate patch location and the patches will not be deployed. The alternate patch location is defined in **Patching > VCM Patching Administration > Machine Group Mapping > Local Patch Path**.

Default Location for UNIX/Linux Patches

If you do not define an alternate location for the patches using Machine Group Mapping, the default location of `/tmp` is used. A temporary expansion of the patches occurs in the `/tmp` directory.

Deploy Patches to UNIX/Linux Machines

Install the patches on UNIX and Linux machines that are managed by VCM Patching.

The deployment assesses whether the patch was installed on the VCM managed machine. The Deploy action exists in the User-created Assessment Template, Imported Template, and Assessment Results for All Bulletins.

Prerequisites

- Verify that your UNIX and Linux machines and operating systems are supported for patch deployment. See the *VCM Hardware and Software Requirements Guide*.
- Ensure that VCM Patching for UNIX/Linux is licensed on the machines.
- Ensure that patch assessments ran successfully.
- Ensure that patches are available locally to the machine.
- Complete the prerequisites. See .

The following procedure deploys the patches using All Bulletins.

Procedure

1. Select **Patching > UNIX/Linux platform > Assessment Results > All Bulletins**.
2. Select the patches to deploy.
3. Select **Deploy**.
4. On the Machines & Bulletins page, review the Recommend Action and Data Age and select the machines and patches to deploy.
5. If you deploy multiple patches, on the Confirm Patch Deployment Order page confirm or reorder the patches in the sequence to be deployed.
6. If you need to set the machine run level, on the Run Level for Patch Installation page, set the run level for the patch installation and keep in mind that in single-user mode no network is available.
7. If you need to specify commands to deploy the patches, on the Command Line Options page specify the options to use.
8. If you need to run remote commands as part of the deployment, on the Pre-Deployment and Post-Deployment Remote Commands page select any of the remote commands to apply during the patch deployment.

9. On the Patch Deployment Schedule page, set the timing for the patch deployment job.
10. On the Reboot Options page, select the options to reboot the machine and send a message or select to avoid a reboot.
11. On the Confirmation page, confirm the patch summary information and complete the wizard to deploy the patch.

After you deploy patches, VCM collects assessment data again to confirm the patches were applied.

VCM saves UNIX and Linux patching change actions in the VCM change log. Click **Console** and select **Change Management > VCM or Non VCM Initiated Change > By Data Type > Patch Assessment**. These change actions are available to Compliance and Reports.

IMPORTANT If a failure occurs at any point in the patch deployment job, the System Administrator must check the status of the system, resolve any issues, and then reassess the machines.

How the Deploy Action Works

The Deploy action runs a command from the Collector to the VCM managed machines.

The VCM job command performs the following actions.

- Assesses VCM managed machines to determine whether the patch was installed since the last assessment.
- Runs a pre-install script (remote command) if specified.
- Installs the patch that already resides on the VCM managed machine's NFS mounted or local file system.
- Runs a post-install script (remote command) if specified.
- Assesses whether the patch was installed on the VCM managed machine.

The pre-install and post-install scripts used in the Deploy actions are remote commands, which differ from using a VCM remote command to install a patch. The patch assessment and deployment process for UNIX and Linux does not use remote commands. If you choose to deploy a patch using a user-created remote command, be aware that the patch will not be assessed until you run an assessment.

Running VCM Patching Reports

You can run patch status reports on UNIX and Windows machines based on trends, details, template summary, bulletins, affected software products, and patch deployment history.

With real-time assessment reports you can generate SQL reports for machines assessed against bulletins and affected software products. With the patch deployment history report, you can report on the history of patch deployments using VCM Patching assessment results.

You can generate several reports.

- Create real-time assessment reports by bulletins or products.
- Create real-time assessment reports by affected software products.
- Create real-time assessment reports of bulletins and products.
- Create a patch deployment history report.

When you generate reports, you can take the following actions.

- Manually update VCM Patching Windows content.
- Run reports without Internet access.

Customize Your Environment for VCM Patching

Perform routine maintenance on your VCM configuration management database. With routine maintenance, you can tune the visibility of configuration information so that the policies you develop and the actions you take are appropriate for your IT infrastructure.

To ensure that you retain the correct information for auditing, review the data retention settings and update them appropriately according to your policies.

For more information about VCM Patching, see the online help.

Getting Started with Operating System Provisioning 11

Operating system (OS) provisioning is the process of installing operating systems to physical or virtual machines. As part of the provisioning process, you can add newly provisioned machines to VCM.

OS provisioning enables you to quickly deploy one or more physical or virtual machines to meet expanding business needs. Some of these machines may have limited use and lifespan, and may be re-provisioned for other purposes. Other machines are provisioned and distributed for long term use.

The provisioning process installs the supported operating system and the VCM Agent. When the target machines are licensed, you can collect machine data, monitor the machines' state and status, and manage the security and compliance of the machines.

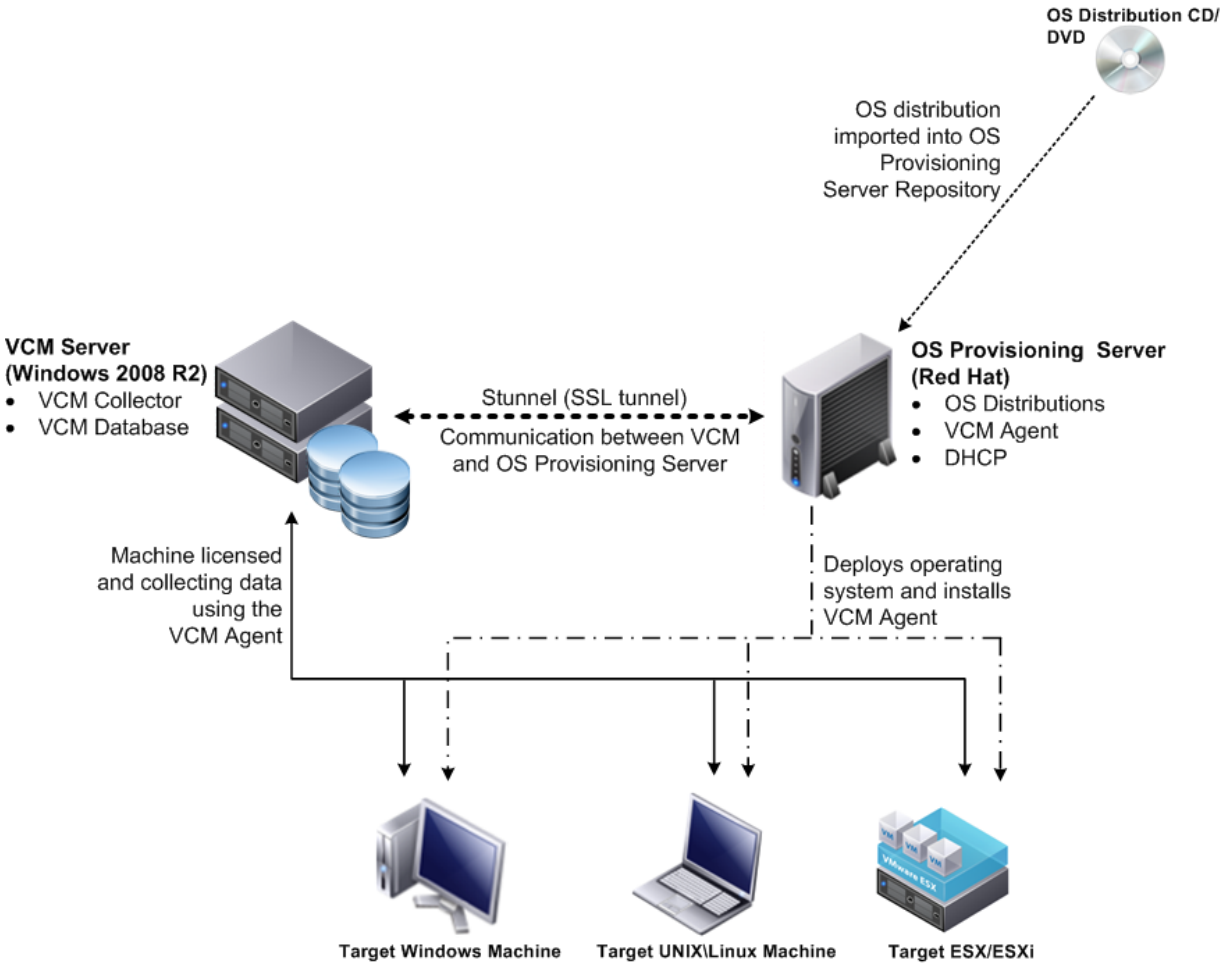
Troubleshooting information is available in the *VCM Troubleshooting Guide*.

OS Provisioning Components

The OS provisioning components include the VCM Collector, the OS Provisioning Server, and the target physical or virtual machines.

The OS Provisioning Server, when it is installed and configured in your environment, serves as the engine for OS provisioning. However, the process of initiating provisioning actions is managed through the VCM Console.

Figure 11–1. Relationship of OS Provisioning Components


OS Distribution CD/ DVD
OS distribution imported into OS Provisioning Server Repository
VCM Server (Windows 2008 R2)
• VCM Collector
• VCM Database
Stunnel (SSL tunnel)
Communication between VCM and OS Provisioning Server
OS Provisioning Server (Red Hat)
• OS Distributions
• VCM Agent
• DHCP
Machine licensed and collecting data using the VCM Agent
Deploys operating system and installs VCM Agent
Target Windows Machine
Target UNIX\Linux Machine
Target ESX/ESXi

How OS Provisioning Works

The process of provisioning operating systems on physical or virtual machines includes actions you run in VCM, actions you perform outside VCM, the underlying processes associated with the actions, and the results.

- You use VCM to collect the available OS distributions from the OS Provisioning Server.

  The collected distributions are displayed in the OS Distributions data grid and are available to install on target machines.

- You set the BIOS on the target machines to network boot.
- You connect the target machines to the provisioning network and turn them on.

  The OS Provisioning Server discovers the available target machines.

- You use VCM to collect the discovered target machines from the OS Provisioning Server.

  The discovered target machines are display in the Provisionable Machines data grid by MAC address.

- You use VCM to send the command to the OS Provisioning Server to provision the target machines.

  The OS Provisioning Server creates an installation session for the target machines based on the configured OS distribution settings.

- You reboot the target machines.

  As each target machine requests an IP address from the DHCP server and requests a PXE boot, OS Provisioning Server checks the machine's MAC address to determine if the machine has an installation session waiting on the OS Provisioning Server. If an installation session for the machine is found, the OS installer boots over TFTP, the OS distribution and VCM Agent are downloaded to the target machines using HTTP, and the distribution and Agent are installed on the target machines.

  When the installation completes, the new physical or virtual machines are displayed in the Provisioned Machines data grid. They are licensed or available to license in VCM. If the machine is not licensed, you must license it to manage the machine. As each machine is licensed, you manage it in VCM as a Window, UNIX/Linux, or ESX machine.

Provision Target Machines with Operating System Distributions

Operating system provisioning includes VCM and the OS Provisioning Server. VCM submits the actions to the OS Provisioning Server, which runs the actions on the target machines.

Prerequisites

Install the OS Provisioning Server and import the OS distributions. See "Installing, Configuring, and Upgrading the OS Provisioning Server and Components" on page 21.

Procedure

1. "Collect OS Distributions" on page 201

   Collect the OS Distributions to ensure that you have access to all the operating systems in the OS Provisioning Server repository.

2. "Discover Provisionable Machines" on page 202

   The OS Provisioning Server identifies provisionable physical or virtual machines in your environment when the target machines set to network boot and attempt to PXE boot.

3. "Provision Machines with Operating System Distributions" on page 202

   The OS provisioning process installs one Windows, UNIX/Linux, or ESX operating system distribution on one or more physical or virtual machines using OS provisioning.

Continuous provisioned machine management is based on the latest data you collect from the OS Provisioning Server. See "Provisioned Machines Results" on page 213.

Collect OS Distributions

Collect the OS Distributions to ensure that you have access to all the operating systems in the OS Provisioning Server repository. These OS Distributions are operating system images that are available to install on target machines.

Prerequisites

- Ensure that operating system distributions are imported into the OS Provisioning Server repository. To import OS distributions, see "Import Distributions into the OS Provisioning Server Repository" on page 33.
- Verify that the OS Provisioning Integration Enabled setting is configured with a value greater than 0. The default value is 5. Click **Administration** and select **Settings > OS Provisioning Settings > OS Provisioning Server**.

Procedure

1. Click **Administration**.
2. Select **Machines Manager > OS Provisioning > OS Distributions**.
3. Click **Refresh**.

   This action collects data from the OS Provisioning Server. When the collection completes, the data grid displays available operating systems distributions.

What to do next

- Verify that the OS Provisioning Server Data Collection job completed. Click **Administration** and select **Job Manager > History > Other Jobs**. Select the time period in which the job ran.
- Discover target machines. See "Discover Provisionable Machines" on page 202.

Discover Provisionable Machines

The OS Provisioning Server identifies provisionable physical or virtual machines in your environment when the target machines set to network boot and attempt to PXE boot.

Prerequisites

- Ensure that the target machines have a minimum of 1 GB RAM and meet the minimum RAM requirements for the operating system you are installing.
- Configure the primary network interface on the target machines with a connection to the OS Provisioning Server deployment network. If you use a different network as the primary interface, the deployment process appears to start, but you receive communication errors and the process ultimately fails.

Procedure

1. On target machines, configure the BIOS to network boot.
2. Start the machines on your provisioning network.
3. In VCM, click **Administration**.
4. Select **Machines Manager > OS Provisioning > Provisionable Machines**.
5. On the data grid toolbar, click **Refresh**.

   This action collects data from the OS Provisioning Server and displays the provisionable machines in the data grid. The machines are identified by MAC address.

What to do next

Provision the target machine. See "Provision Machines with Operating System Distributions" on page 202.

Provision Machines with Operating System Distributions

The OS provisioning process installs one Windows, UNIX/Linux, or ESX operating system distribution on one or more physical or virtual machines using OS provisioning.

- "Provision Windows Machines" on page 203

  Provisioning physical or virtual machines with a Windows operating system installs the selected operating system and the VCM Agent on one or more of your Windows machines.

- "Provision UNIX/Linux Machines" on page 205

  Provisioning physical or virtual machines with a UNIX or Linux operating system installs the selected operating system and the VCM Agent on one or more of your UNIX/Linux machines.

- "Provision ESX Machines" on page 211

  Provisioning physical or virtual machines with an ESX operating system installs the selected operating system on one or more of your ESX machines.

Provision Windows Machines

Provisioning physical or virtual machines with a Windows operating system installs the selected operating system and the VCM Agent on one or more of your Windows machines.

You can install one OS distribution on one or more target machines. To install a different OS distribution, configure a new OS provisioning action.

Prerequisites

- Verify that the operating system you are installing is compatible with the hardware or configuration of the target physical or virtual machines. For example, the operating system must support the drivers required by the hardware.
- Verify that the OS distributions are collected and appear in the OS Distributions data grid. See "Collect OS Distributions" on page 201.
- Verify that the target machines are discovered and appear in the Provisionable Machines data grid. See "Discover Provisionable Machines" on page 202.
- (Optional) Identify or create any post-install scripts that you want to run on the target machine after it is provisioned with the new operating system. The post-install scripts are copied to the target machine along with the OS distribution and runs after the operating system is installed.

Procedure

1. Click **Administration**.
2. Select **Machines Manager > OS Provisioning > Provisionable Machines**.
3. Select one or more target machines in the data grid on which you are installing the same OS distribution.
4. Click **Provision**.
5. On the Select Machines page, add or remove target machines from the selected machine list and click **Next**.

6. On the Select OS Distribution page, select the Windows operating system you are installing on the selected machines and click **Next**.
7. On the Settings page, configure the options required for your selected Window OS distribution and click **Next**.

Field	Description
Product License Key	(Optional for Windows 2008. Required for Windows 2003 and Windows 7.) Type a license matching the operating system you are installing.
License Key Type	(Required for Windows 2003 and Windows 7, and for Windows 2008 if Product License Key is provided.) Select the license type, either Retail or MAK (multiple activation key).
Admin Password	(Required) Type the password for the target machines' local Administrator account.
Re-enter Admin Password	(Required) Retype the password.
Domain or Workgroup	(Required) If a Domain and Domain User are specified, Domain details are used. If the domain details are not provided, then the Workgroup is used.
Add machine(s) to a Domain	Select the check box to add the machines to a Domain rather than a Workgroup. If you select this option, you must configure the domain details.
Domain Type	(Available if you select Add machine(s) to a Domain) Select the type in the drop-down list.
Domain User	(Available if you select Add machine(s) to a Domain) Type a user name.
Domain User Password	(Available if you select Add machine(s) to a Domain) Type a password for the specified Domain User.
Re-enter Domain User Password	(Available if you select Add machine(s) to a Domain) Retype the password.
Organization	Name of the licensing organization.
Windows SKU	(Window 2008 and Windows 7 only) Select the value in the drop-down list. See the online help for possible values.
Use DHCP to determine IP address	Select this option to use your designated DHCP to assign IP address, subnet, default gateway, and DNS. If not selected, you must manually add the information on the Machine-Specific Settings page.
License these machines for VCM	Select the option to automatically licenses the machines for VCM management.

8. On the Machine-Specific Settings page, type the **HostName** and click **Next**.

   The HostName is limited to 15 characters.

   If you did not select **Use DHCP to determine IP address** on the Settings page, you are required to configure the IP Address, Subnet, Default Gateway, and DNS.

9. (Optional) On the Post-install Script page, type a **Script Name** and the script, and click **Next**.

10. (Optional) On the Disk Configuration page, select one of the options and click **Next**.

Option	Description
Use all available disk space	Does not partition the disk.
Create partition with *nn* GB.	Partitions and formats the specified space. The space you specify must be less than the total available space.

11. On the Confirmation page, click **Finish**.

    The OS Provisioning Server starts jobs for each of the selected target machines. Each job creates a configured session for the specified machines. The configured session includes information about the target machine, the OS distribution, the configuration information for the selected combination of target machine and operating system, and the VCM Agent.

12. Reboot the target machines.

    You must cycle the power on the machines either manually or using some remote administration mechanism. The machines must be configured to network boot from the OS Provisioning Server, which identifies the configured session that is waiting and the installation begins. If the session does not exist, then the target machine remains provisionable and is not provisioned until a session is created and the target machine is rebooted.

What to do next

- Verify that the provisioning process has begun. Click Administration and select **Machines Manager > OS Provisioning > Provisionable Machines**. The machines are also displayed in the appropriate Available Machines or Licensed Machines data grid with an OS provisioning status of OS Provisioning Queued.
- Verify that the provisioning process is completed. Click **Administration** and select **Machines Manager > OS Provisioning > Provisioned Machines**. The OS provisioning status is OS Provisioning Succeeded or OS Provisioning Overwritten.
- Configure the Windows 2008 SP2, and R2, and Windows 7 machines on a public network with access to the Internet and manually complete the Windows license activation on the provisioned machines.
- (Optional) Change the Agent communication protocol. See "Change Agent Communication" on page 211.

Provision UNIX/Linux Machines

Provisioning physical or virtual machines with a UNIX or Linux operating system installs the selected operating system and the VCM Agent on one or more of your UNIX/Linux machines.

You can install one OS distribution on one or more target machines. To install a different OS distribution, configure a new OS provisioning action.

Prerequisites

- Verify that the operating system you are installing is compatible with the hardware or configuration of the target physical or virtual machines. For example, the operating system must support the drivers required by the hardware.
- Verify that the OS distributions are collected and appear in the OS Distributions data grid. See "Collect OS Distributions" on page 201.
- Verify that the target machines are discovered and appear in the Provisionable Machines data grid. See "Discover Provisionable Machines" on page 202.
- (Optional) Identify or create any post-install scripts that you want to run on the target machine after it is provisioned with the new operating system. The post-install scripts are copied to the target machine along with the OS distribution and runs after the operating system is installed.

Procedure

1. Click **Administration**.
2. Select **Machines Manager > OS Provisioning > Provisionable Machines**.
3. Select one or more target machines in the data grid on which you are installing the same OS distribution.
4. Click **Provision**.
5. On the Select Machines page, add or remove target machines from the selected machine list and click **Next**.

6. On the Select OS Distribution page, select the a UNIX or Linux operating system you are installing on the selected machines and click **Next**.
7. On the Settings page, configure the options required for your selected UNIX or Linux OS distribution and click **Next**.

Option	Description
Product License Key	Type the license to use when installing the operating system on the target machines. The license must match the operating system you are installing.
Root Password	(Required) Type the password you are assigning to the local root.
Re-enter Root Password	(Required) Retype the password.
Domain	(Required) Type the domain to which you are assigning the machines.
Use DHCP to determine IP address	Select this option to use your designated DHCP to assign IP address, subnet, default gateway, and DNS. If this option is not selected, you must manually enter the information on the Machine-Specific Settings page.
License these machines for VCM after deployment	Select this option to automatically license the target machines for VCM management.

8. On the Machine-Specific Settings page, type the **HostName** and click **Next**.

   The HostName is limited to 32 characters.

   If you did not select **Use DHCP to determine IP address** on the Settings page, you are required to configure the IP Address, Subnet, Default Gateway, and DNS.
9. (Optional) On the Post-Install Script page, type a **Script Name**, the script, and click **Next**.

   Post-install scripts are copied to the machine when the OS distribution is copied and runs after the operating system is installed.
10. (Optional) On the Disk Configuration page, configure the options and click **Next**.

    You can either install the operating system without partitioning the disk, or you can create partitions and specify the size.

Option	Description
Custom Volume Plan	Select the check box to partition the disk.
Mount Point	Type the location of the mount point for the partition. For example, `/`, `/boot`, `/usr`, `/var/log`. You use the first partition for the operating system and then specify a second mount point for user home directories. The mount points value must meet the specific criteria.

Option	Description
	■ / and /boot are required mount points. ■ Duplicate mount points are not allowed. ■ For a swap partition, the mount point and the file system type should be swap. ■ When naming mount points, you can use letters, digits, ., -, _, and +. Spaces are not allowed.
Volume Name	Type the name of the logical partition. For example, LogVol00. The volume names must meet specific criteria. ■ When naming volumes, you can use letters, digits, ., or _. Spaces are not allowed. ■ The name limit 16 characters. ■ If you assign a volume name, you must assign a volume group name. ■ If you assign more than one volume name in a volume group, you cannot use the same name for each volume name.
Volume Size	The the size of the partition in megabytes or gigabytes. For example, 10MB or 1GB. If you select **Grow partition to use all remaining space**, you can specify a value of 0MB. If Grow is not selected, you must specify a valid partition size.

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>File System</td><td>Select the type of file system.
For a swap partition, the mount point and the file system type should be swap.
Supported File System options by operating system.

<table>
<tr><th>Operating System</th><th>Supported File System</th><th>swap</th><th>/boot</th><th>/</th><th>/home, /tmp, /usr, /var, /usr/local</th></tr>
<tr><td>RHEL 6.0</td><td>ext2, ext3, ext4, swap, vfat, xfs</td><td>swap</td><td>ext2, ext3, ext4</td><td>ext2, ext3, ext4</td><td>ext2, ext3, ext4,xfs</td></tr>
<tr><td>RHEL 5.4 and 5.5</td><td>ext2, ext3, ext4, swap, vfat</td><td>swap</td><td>ext2, ext3</td><td>ext2, ext3, ext4</td><td>ext2, ext3, ext4</td></tr>
<tr><td>RHEL 5.0 and 5.2</td><td>ext2, ext3, swap, vfat</td><td>swap</td><td>ext2, ext3</td><td>ext2, ext3</td><td>ext2, ext3</td></tr>
<tr><td>SLES 10.0 and 11.1</td><td>reiser, ext2, ext3, xfs, jfs, swap</td><td>swap</td><td>reiser, ext2, ext3, xfs, jfs</td><td>reiser, ext2, ext3, xfs, jfs</td><td>reiser, ext2, ext3, xfs, jfs</td></tr>
</table>
</td></tr>
<tr><td>Volume Group Name</td><td>Type the name of the logical group.
For example, VolGroup00. You can specify only one volume group on the target machines. You may add volume groups after the OS distribution is installed.
The volume names must meet specific criteria.
■ When naming volumes, you can use letters, digits, ., or _. Spaces are not allowed.
■ The name limit 16 characters.
■ If you assign a volume name, you must assign a volume group name.
■ (SLES only) You can assign only one volume group when partitioning the disk.
■ (RHEL 5.x and 6.0, and SLES 10.3 and 11.1 only) You cannot use /boot as part of the volume group name.</td></tr>
<tr><td>Add</td><td>Click to add the configuration data to the Custom Volume Plan list.</td></tr>
<tr><td>Custom Volume Plan list</td><td>Displays the disk configuration data.</td></tr>
</table>

Option	Description
Grow partition to use all remaining space	Select the option to allow the logical volume to fill available space up to the maximum size specified for the volume. You can select the option for only one partition. If you select this option, you can specify a Volume Size of 0MB.
Remove	Click to delete the selected row from the custom volume plan list.

11. On the Confirmation page, click **Finish**.

    The OS Provisioning Server starts jobs for each of the selected target machines. Each job creates a configured session for the specified machines. The configured session includes information about the target machine, the OS distribution, the configuration information for the selected combination of target machine and operating system, and the VCM Agent.

12. Reboot the target machines.

    You must cycle the power on the machines either manually or using some remote administration mechanism. The machines must be configured to network boot from the OS Provisioning Server, which identifies the configured session that is waiting and the installation begins. If the session does not exist, then the target machine remains provisionable and is not provisioned until a session is created and the target machine is rebooted.

What to do next

- Verify that the provisioning process has begun. Click Administration and select **Machines Manager > OS Provisioning > Provisionable Machines**. The machines are also displayed in the appropriate Available Machines or Licensed Machines data grid with an OS provisioning status of OS Provisioning Queued.
- Verify that the provisioning process is completed. Click **Administration** and select **Machines Manager > OS Provisioning > Provisioned Machines**. The OS provisioning status is OS Provisioning Succeeded or OS Provisioning Overwritten.
- Move the UNIX/Linux machine to your production network and synchronize the network time. See "Synchronize Time on Installed Linux Operating Systems" on page 210.
- (Optional) Change the Agent communication protocol. See "Change Agent Communication" on page 211.

Synchronize Time on Installed Linux Operating Systems

When Linux machines are provisioned with an operating system, the Network Time Protocol (NTP) service is not running. After moving the newly provisioned Linux machines to a network with access to the NTP server, you must synchronize the time on the machines to network time.

Prerequisites

- Configure the Linux machines on a network with access to the NTP server.
- Identify the NTP servers used in your environment.

Procedure

1. On the Linux machine, log in as `root`.
2. Run the `ntpdate -u <ntpserver>` command to update the machine clock.

   For example, `ntpdate -u ntp-time.for.mydomain`.
3. Open the `/etc/ntp.conf` file and add the NTP servers used in your environment.

   You can add multiple NTP servers similar to these examples.

   ```
   server ntp-time.for.mydomain

   server otherntp.server.org

   server ntp.research.gov
   ```
4. Run the `service ntpd start` command to start the NTP service and implement you configuration changes.

Change Agent Communication

The VCM Agent is installed by the OS Provisioning Server with default settings. After the operating system distribution is installed, you can change the communication setting or install a new Agent.

Prerequisites

Install Windows or UNIX/Linux operating system distribution. See "Provision Windows Machines" on page 203 or "Provision UNIX/Linux Machines" on page 205.

Procedure

1. (Optional) Configure the communication settings for the machines on which you installed one of the following operating using OS provisioning.
   - The Windows Agent is installed with DCOM as the communication protocol. To change the protocol, click **Administration** and then select **Machines Manager > Licensed Machines > Licensed Windows Machines > Change Protocol**.
   - The UNIX/Linux Agents are installed with inetd or xinetd, as appropriate, with a default communication port of 26542. If you want to change any Agent settings, you must uninstall the Agent from the machine, and then reinstall it with the settings you require. See "Install the Agent on UNIX/Linux Machines" on page 114.

Provision ESX Machines

Provisioning physical or virtual machines with an ESX operating system installs the selected operating system on one or more of your ESX machines.

You can install one OS distribution on one or more target machines. To install a different OS distribution, configure a new OS provisioning action.

Prerequisites

- Verify that the operating system you are installing is compatible with the hardware or configuration of the target physical or virtual machines. For example, the operating system must support the drivers required by the hardware.
- Verify that the OS distributions are collected and appear in the OS Distributions data grid. See "Collect OS Distributions" on page 201.

- Verify that the target machines are discovered and appear in the Provisionable Machines data grid. See "Discover Provisionable Machines" on page 202.

Procedure

1. Click **Administration**.
2. Select **Machines Manager > OS Provisioning > Provisionable Machines**.
3. Select one or more target machines in the data grid on which you are installing the same OS distribution.
4. Click **Provision**.
5. On the Select Machines page, add or remove target machines from the selected machine list and click **Next**.
6. On the Select OS Distribution page, select the ESX operating system you are installing on the selected machines and click **Next**.
7. On the Settings page, configure the options required for your selected ESX OS distribution and click **Next**.

Option	Description
Product License Key	Type the license to use when installing the operating system on the target machines. The license must match the operating system you are installing.
Root Password	(Required) Type the password you are assigning to the local root.
Re-enter Root Password	(Required) Retype the password.
Domain	(Required) Type the domain to which you are assigning the machines.
Use DHCP to determine IP address	Select this option to use your designated DHCP to assign IP address, subnet, default gateway, and DNS. If this option is not selected, you must manually enter the information on the Machine-Specific Settings page.
License these machines for VCM after deployment	Select this option to automatically license the target machines for VCM management.

8. On the Machine-Specific Settings page, type the **HostName** and click **Next**.

   The HostName is limited to 32 characters.

   If you did not select **Use DHCP to determine IP address** on the Settings page, you are required to configure the IP Address, Subnet, Default Gateway, and DNS.

9. On the Confirmation page, click **Finish**.

   The OS Provisioning Server starts jobs for each of the selected target machines. Each job creates a configured session for the specified machines. The configured session includes information about the target machine, the OS distribution, the configuration information for the selected combination of target machine and operating system, and the VCM Agent.

10. Reboot the target machines.

    You must cycle the power on the machines either manually or using some remote administration mechanism. The machines must be configured to network boot from the OS Provisioning Server, which identifies the configured session that is waiting and the installation begins. If the session does not exist, then the target machine remains provisionable and is not provisioned until a session is created and the target machine is rebooted.

What to do next

- Verify that the provisioning process has begun. Click Administration and select **Machines Manager > OS Provisioning > Provisionable Machines**. The machines are also displayed in the appropriate Available Machines or Licensed Machines data grid with an OS provisioning status of OS Provisioning Queued.
- Verify that the provisioning process is completed. Click **Administration** and select **Machines Manager > OS Provisioning > Provisioned Machines**. The OS provisioning status is OS Provisioning Succeeded or OS Provisioning Overwritten.
- Configure the host settings for the provisioned ESX machines. See "Configure ESX and ESXi Machines After OS Provisioning" on page 213.

Configure ESX and ESXi Machines After OS Provisioning

Configure the host settings for ESX and ESXi machines after the OS provisioning process installs the operating system so that you can begin managing the ESX machines in VCM.

Prerequisites

Install an ESX or ESXi operating system distribution on one or more target machines. See "Provision ESX Machines" on page 211.

Procedure

1. Depending on whether you selected **License these machines for VCM** during provisioning, use one of these options to ensure the ESX or ESXi machine is licensed in VCM.
   - If you licensed the machine during OS provisioning, you must configure the host settings. Click **Administration** and select **Machines Manager > Licensed Machines > Licensed VM Hosts > Change Settings**
   - If not licensed during OS provisioning, you must license and configure the host settings. Click **Administration** and select **Machines Manager > Available Machines > Available VM Hosts > License**.

What to do next

Configure the ESX or ESXi machines to be managed . See "Configure Virtual Machine Host Collections" on page 147.

Provisioned Machines Results

Review the OS provisioning data that is specific to the provisioning process.

After you provision the target machines, VCM manages them as Window, UNIX/Linux, or ESX/VM Host machines. As managed machines, you collect data, add software, run patching assessments, and apply rules to maintain machine compliance in your environment.

The displayed data is only as current as the last time you collected from the OS Provisioning Server.

Option	Description
Administration	View administrative details about the OS Provisioning Server. ■ To view all provisioned machines, click **Administration** and select **Machines Manager > OS Provisioning > Provisioned Machines**. ■ To view the provisioned Windows machines, click **Administration** and select **Machines Manager > Licensed Machines > Licensed Windows Machines**. The OS Provisioning Status column indicates whether the Windows machine was create using OS provisioning. ■ To view the provisioned UNIX/Linux machines, click **Administration** and select **Machines Manager > Licensed Machines > Licensed UNIX Machines**. The OS Provisioning Status column indicates whether the UNIX/Linux machine was create using OS provisioning. ■ To view the provisioned ESX machines, click **Administration** and select **Machines Manager > Licensed Machines > Licensed VM Hosts Machines**. The OS Provisioning Status column indicates whether the ESX or ESXi machine was create using OS provisioning.

Re-Provision Machines

You can re-provision Windows, UNIX/Linux, or ESX machines where the operating system was installed using the OS Provisioning Server and VCM.

When machines are re-provisioned, you may change the machine name.

CAUTION Re-provisioning overwrites the existing disk with a new operating system. All existing data is lost.

Prerequisites

- Verify that the machine to be re-provisioned is listed in the Provisioned Machines data grid. Select **Administration** and click **Machines Manager > OS Provisioning > Provisioned Machines**.
- Review the provisioning process for the OS distribution you are installing. See "Provision Machines with Operating System Distributions" on page 202.
- On the target machine, set the BIOS to network boot.

Procedure

1. Click **Administration**.
2. Select **Machines Manager > OS Provisioning > Provisioned Machines**.
3. Select the machines.
4. Click **Re-provision**.
5. On the **Select Machines** page, add or remove machines and click **Next**.
6. On the **Select OS Distribution** page, select the operating system you are installing on the selected machines and click **Next**.
7. Continue with the provisioning wizard.

   The wizard options vary depending on the OS distribution you are installing.
8. When you are certain that the selected machines are those you want to re-provision, select the **Proceed with re-provisioning of the operating system on the selected machines** check box.
9. Click **Finish**.

   The OS Provisioning Server starts jobs for each of the selected machines. Each job creates a configured session for the specified machines. The configured session includes information about the target machine, the OS distribution, the user configuration information for the selected combination of machine and operating system, and the VCM Agent.
10. Reboot the target machines.

    You must the cycle the power on the machines either manually or using some remote administration mechanism. The machines must be configured to network boot from the provisioning network. If a session is waiting on the OS Provisioning Server, the installation begins. If the session does not exist, then the machine remains provisioned and will not be re-provisioned until the session is created.

What to do next

- Verify that the provisioning process has begun. Click Administration and select **Machines Manager > OS Provisioning > Provisionable Machines**. The machines are also displayed in the appropriate Available Machines or Licensed Machines data grid with an OS provisioning status of OS Provisioning Queued.
- Verify that the provisioning process is completed. Click **Administration** and select **Machines Manager > OS Provisioning > Provisioned Machines**. The OS provisioning status is OS Provisioning Succeeded or OS Provisioning Overwritten.
- Configure the Windows 2008 SP2, and R2, and Windows 7 machines on a public network with access to the Internet and manually complete the Windows license activation on the provisioned machines.
- Configure the host settings for the provisioned ESX machines. See "Configure ESX and ESXi Machines After OS Provisioning" on page 213.
- (Optional) Change the Agent communication protocol. See "Change Agent Communication" on page 211.

Getting Started with Software Provisioning 12

Software provisioning is the process you use to create software packages, publish the packages to repositories, and then install packages on one or more target machines.

To support the provisioning process, the VCM Software Provisioning components consist of VMware vCenter Configuration Manager Package Studio, software package repositories, and Package Manager.

For more information about software provisioning, see VCM online Help, the *VCM Software Provisioning Components Installation and User's Guide*, and the Package Studio online Help.

Using Package Studio to Create Software Packages and Publish to Repositories

Package Studio is the application used to build software packages for installation on target Windows servers and workstations.

Windows packages can include in-house and commercial software installation files, including .msi, .exe, VBScripts, python, PowerShell.

To add a software installer to a package, it must be able to install and uninstall unmanned or quietly using command line options, response files, or other similar methods.

Software Repository for Windows

Software Repository for Windows is the shared location to which packages are published by Package Studio and the location from which Package Manager downloads packages for installation.

Package Manager for Windows

Package Manager is the application installed on each machine to manage the installation and removal of the software contained in packages. Package Manager is configured to use one or more repositories as sources for packages.

If you are using the software provisioning components in conjunction with VMware vCenter Configuration Manager (VCM), you can use VCM to add and remove sources, and to install and remove packages.

Software Provisioning Component Relationships

The following diagram displays the general relationship between Package Studio, repositories, and Package Manager in a working environment.

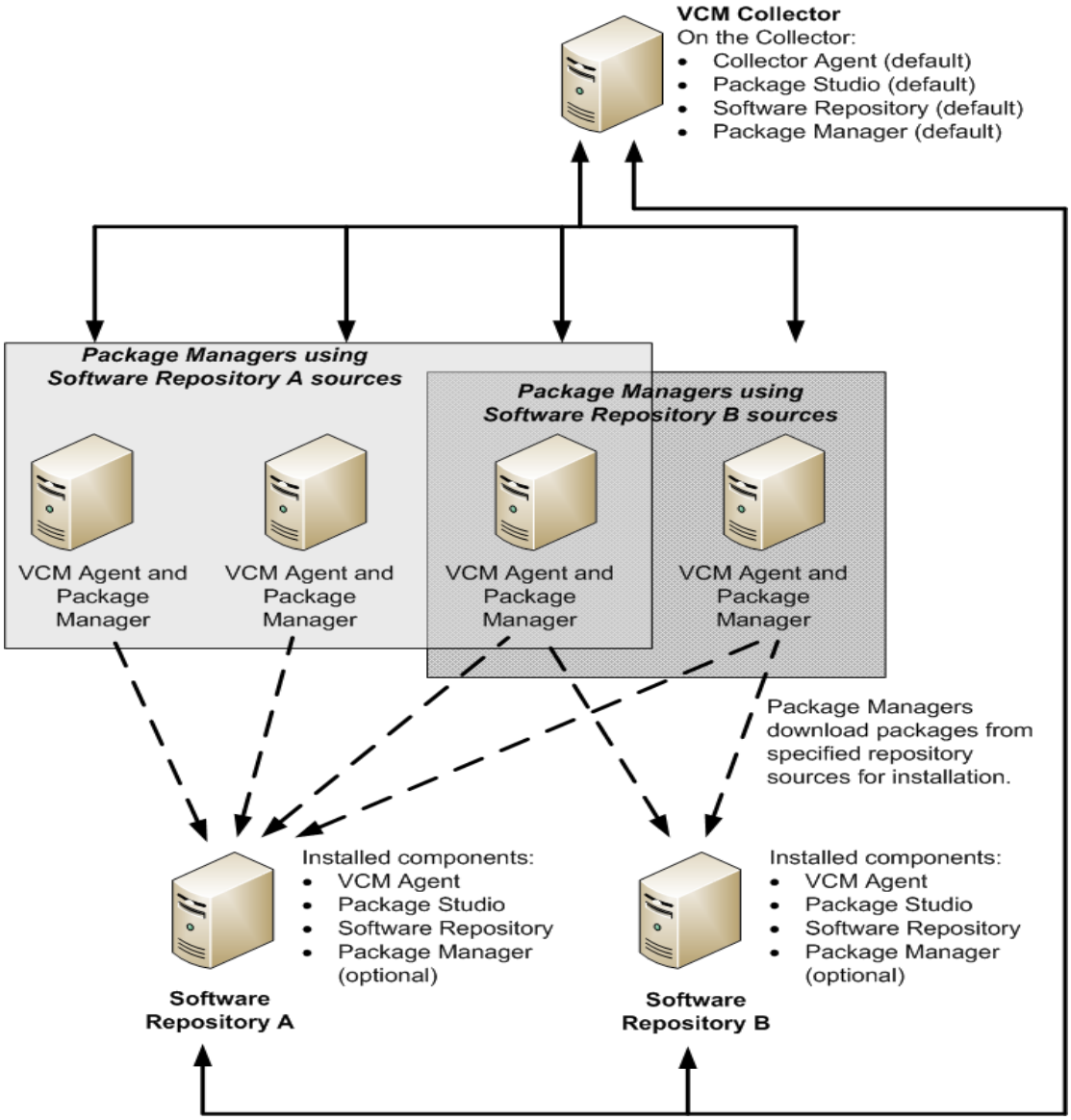


Figure 12–1. Software Provisioning Diagram

Install the Software Provisioning Components

The software provisioning components are installed on the VCM Collector by default. VMware recommends that you install the Software Repository for Windows and the VMware vCenter Configuration Manager Package Studio on a machine other than the Collector.

The software provisioning components should be installed on machines with these relationships:

- **Software Repository for Windows:** Installed on at least one Windows machine in your environment, and installed on the same machine with Package Studio. Install the repository before installing Package Studio.
- **VMware vCenter Configuration Manager Package Studio:** Installed on the same machine as your software repository.
- **Package Manager:** Installed on all Windows machines on which you are managing software provisioning.

To uninstall the applications using a script at a later date, you should save a copy of each of the .msi files in an archive location. To uninstall using the .msi, you must have the same version used to install the application.

Procedure

1. "Install Software Repository for Windows" on page 219

   The Software Repository for Windows and the VMware vCenter Configuration Manager Package Studio should be installed on the same machine. Installing the repository installs the Repository folders and subfolders, and configures the virtual directory. The virtual directory is used by Package Manager to access the repository.

2. "Install Package Studio" on page 220

   The VMware vCenter Configuration Manager Package Studio and the repository must be installed on the same machine. The process installs the application files and specifies the repository to which Package Studio will publish packages.

3. "Install Package Manager on Managed Machines" on page 222

   The Package Manager, which installed on the target machines, manages the installation of the software packages. It does not contain the software packages, only pointers to the packages in the repository sources of which it is aware.

Install Software Repository for Windows

The Software Repository for Windows and the VMware vCenter Configuration Manager Package Studio should be installed on the same machine. Installing the repository installs the Repository folders and subfolders, and configures the virtual directory. The virtual directory is used by Package Manager to access the repository.

Prerequisites

- Verify that the target machine meets the supported hardware, operating system, and software requirements. See *VCM Hardware and Software Requirements Guide* for currently supported platforms and requirements.
- Ensure that you have access to the `Repository.msi`, which is available on the VMware Web site or in the vCenter Configuration Manager application files.The default location in the VCM application files is `C:\Program Files (x86)\VMware\VCM\AgentFiles\Products`.

Procedure

1. Double-click `Repository.msi`.
2. On the Welcome page, click **Next**.
3. Review the license agreement, select the appropriate options to continue, and click **Next**.
4. On the Installation Folder page, use the default path or click **Change** to modify the path.

   When the path is correct, click **Next**.
5. On the Virtual Directory page, use the default name or type a new name in the text box, and click **Next.**.
6. On the Ready to Install page, click **Install**.
7. When the Setup Completes page appears, click **Finish**.

The repository and the virtual directory are added to the locations specified during installation. The default location for the repository is `C:\Program Files\VMware\VCM\Tools\Repository` (on 32-bit machines) or `C:\Program Files (x86)\VMware\VCM\Tools\Repository` (on 64-bit machines). The default virtual directory SoftwareRepository is added to **Internet Information Services (IIS) > Web Sites > Default Web Site**.

Manually Uninstall the Repository

Using the following command line syntax, you can run an unattended uninstall the software repository.

Prerequisites

- To uninstall the application, you must use the same version of the `Repository.msi` that was used to install the application.

Procedure

1. Copy the `Repository.msi` to the machine on which you are uninstalling the application or point to the file in a shared directory.
2. Run the .msi file using the following command line syntax:

   ```
   msiexec /x [path]\Repository.msi /l*v %temp%\Repository.log
   ```

Install Package Studio

The VMware vCenter Configuration Manager Package Studio and the repository must be installed on the same machine. The process installs the application files and specifies the repository to which Package Studio will publish packages.

Prerequisites

- Verify that the target machine meets the supported hardware, operating system, and software requirements. See *VCM Hardware and Software Requirements Guide* for currently supported platforms and requirements.
- Ensure you have access to the `PackageStudio.msi`, which is available on the VMware Web site or in the vCenter Configuration Manager application files. The default location in the VCM application files is `C:\Program Files (x86)\VMware\VCM\AgentFiles\Products`.
- (Recommended) Software Repository for Windows is installed. Installing the repository before installing Package Studio will reduce the manual configuration steps.

Procedure

1. Double-click `PackageStudio.msi`.
2. On the Welcome page, click **Next**.
3. Review the license agreement, select the appropriate options to continue, and click **Next**.
4. On the Installation Folder page, use the default path or click **Change** to modify the path, and click **Next**.
5. On the Repository Root Folder page, verify the path is to your installed repository files.

   If the path is not accurate, click **Change**. When the path is correct, click **Next**.
6. On the Ready to Install page, click **Install**.
7. On the Setup Complete page, click **Finish**.

The Package Studio is installed to the location specified during installation. The default location is `C:\Program Files\VMware\VCM\Tools\Package Studio` (on 32-bit machines) or `C:\Program Files (x86)\VMware\VCM\Tools\Package Studio` (on 64-bit machines).

To start Package Studio, click **Start** and select **All Programs > VMware vCenter Configuration Manager > Tools > Package Studio**, or open the Package Studio folder and double-click **PackageStudio.exe**.

Install Package Studio Using Unattended .MSI

The manual installation process installs the application files and specifies the repository to which Package Studio will publish packages.

Prerequisites

- Verify that the target machine meets the supported hardware, operating system, and software requirements. See *VCM Hardware and Software Requirements Guide* for currently supported platforms and requirements.
- Ensure you have access to the `PackageStudio.msi`, which is available on the VMware Web site or in the vCenter Configuration Manager application files. The default location in the VCM application files is `C:\Program Files (x86)\VMware\VCM\AgentFiles\Products`.
- (Recommended) Software Repository for Windows is installed. Installing the repository before installing Package Studio will reduce the manual configuration steps.

Procedure

1. On your Collector, go to `C:\Program Files (x86)\VMware\VCM\AgentFiles\Products`.
2. Locate the `PackageStudio.msi` file and copy it to the target machine.

   You can also run the .msi from a shared location.
3. On the target machine, run the .msi file using the following command line syntax.

   ```
   msiexec /i [path]\PackageStudio.msi /qn /l*v %temp%\PackageStudio.log
   ```

You can add the following arguments if you want to specify locations other than the default directories:

`REPOSITORY_ROOT=C:\Program Files (x86)\VMware\VCM\Tools\Repository\` (Defaults to this or uses the Repository's value if it is already installed)

`PACKAGESTUDIO_DIR="C:\Program Files (x86)\VMware\VCM\Tools\Package Studio\"` (defaults to this path)

The Package Studio is installed to the location specified during installation. The default location is `C:\Program Files\VMware\VCM\Tools\Package Studio` (on 32-bit machines) or `C:\Program Files (x86)\VMware\VCM\Tools\Package Studio` (on 64-bit machines).

To start Package Studio, click **Start** and select **All Programs > VMware vCenter Configuration Manager > Tools > Package Studio**, or open the Package Studio folder and double-click **PackageStudio.exe**.

Manually Uninstall Package Studio

Use the following script to run an unattended uninstall the Package Manager.

Prerequisites

- To uninstall the application, you must use the version of the `PackageStudio.msi` that was used to install the application.

Procedure

1. Copy the `PackageStudio.msi` to the machine on which you are uninstalling the application. You can also run it from a shared location.
2. Run the installation file using the following command line syntax:

```
msiexec /x [path]\PackageStudio.msi /l*v %temp%\PackageStudio.log
```

When Package Studio is uninstalled from a machine, the locally saved projects and `.crate` files remain on the machine, allowing you to copy them to another machine or to delete them manually if they are not needed.

Install Package Manager on Managed Machines

The Package Manager, which installed on the target machines, manages the installation of the software packages. It does not contain the software packages, only pointers to the packages in the repository sources of which it is aware. When directed to install, the package is copied from the repository to the cratecache folder on the target machines. It is from this location that Package Manager upzips the files to the %TMP% directory and runs the configured installation.

The Package Manager is automatically installed on target machines when the 5.3 VCM Agent or later is installed.

When a Remove Package action is sent to Package Manager, it checks first for the package in the cratecache. If it is not found, it then checks the repository sources for the package, and again copies it to the target machine's `cratecache folder`. It is from this location that it unzips the files. The configured uninstall files may be run form the zip directory.

Installing the VCM Agent

If you are preparing to use software provisioning on machines not previously managed in VCM, you must first install the VCM Agent. See "Install the VCM Windows Agent on Your Windows Machines" on page 83 for complete instructions. By default, the VCM Agent installation installs the agent extensions for provisioning and the Package Manager for Windows. This default action is based on the settings in **Administration > Settings > General Settings > Installer**.

Prerequisites

- Verify that the target machine meets the supported hardware, operating system, and software requirements. See *VCM Hardware and Software Requirements Guide* for currently supported platforms and requirements.

Verifying the Installation of the Agent Extensions for Provisioning

If you do not know if the machines are ready to use provisioning or not, you can verify the version of the Agent Extensions for Provisioning. The Agent Extensions for Provisioning include the Package Manager.

1. Select **Administration > Machines Manager > Licensed Machines > Licensed Windows Machines**.
2. In the data grid, locate the machines on which you are verifying the existence of the necessary Agent Extensions, and then verify that the Agent Ext. For Prov. Version column contains a value of 5.3 or later. If it does not, you need to either install or upgrade the VCM Agent.

Upgrading the VCM Agent

If an earlier VCM Agent is installed on your machines, you will need to upgrade to the latest Agent. See Upgrade Agent in the online Help.

Using Package Studio to Create Software Packages and Publish to Repositories

Package Studio is the application used to build software packages for installation on target Windows servers and workstations.

Windows packages can include in-house and commercial software installation files, including .msi, .exe, VBScripts, python, PowerShell.

To add a software installer to a package, it must be able to install and uninstall unmanned or quietly using command line options, response files, or other similar methods.

Creating Packages

You use Package Studio to create packages, including the installation files and the required metadata. When the package is ready for use, you publish it to a repository. The procedure here is only a general process. See the Package Studio online Help or the *VCM Software Provisioning Installation and User's Guide* for the detailed procedures.

Procedure

1. Start the VMware vCenter Configuration Manager Package Studio. Select **Start > All Programs All > VMware vCenter Configuration Manager > Tools > Package Studio**.

   NOTE If you are running Package Studio on the Collector or a Windows 2008 Server, you must run the application as administrator. See "Run Package Studio as Administrator" on page 225 for more information.

2. Click **Manage Packages**. Configure the package contents based on the options on the following tabs:
   a. Click **Properties** and type a Name, Version, Description, and select the Architecture. These fields are required. You have the option to update the other fields, depending on you requirements.

      Configuring the package with Depends, Conflicts, Provides, and adding and configuring the installation and removal files.

   b. Click **Files** and import the installation files, add pre-command files, configure the commands and arguments, and add post-command files.
   c. Click **Save** to save the setting and files as a Project (*.prj).
   d. Click **Generate** to save the project as a package (*.crate).
3. Click **Package Signing** and sign the package with a signing certificate.
   a. Click **Open** to select a package (*.crate file).
   b. Click **Sign** and select a certificate from the certificate store or from a file.
4. Click **Manage Repositories** and select the platforms and sections to which you are publishing the package.
   a. Click **Add Platforms** to add a platform.
   b. Select a platform, and then click **Add Sections**.
   c. Select a section, and then click **Publish Package**.
   d. Select the package (.crate) and click **Open**.
   e. (Optional) Select additional platforms and sections to which to publish the package.
   f. Click **Publish**. The package is published to the software repository.
5. Click **External Software** and add externally managed software, especially any packages specified as depends or conflicts in any of your packages.
   a. Click **New External Package** and replace the text with the name you will use as an external software package name.
   b. Type a version number in the Version text box.
   c. Select the **Architecture** in the drop-down list.
   d. Click **Select Attribute Name** and select a registry property or WMI attribute in the drop-down list.
   e. Add attributes.
   f. To save a copy locally, click **Save** .
   g. Click **Publish External SW** to publish to the repository.

Run Package Studio as Administrator

The enhanced security on Windows 2008 Server requires you to run Package Studio as an administrator. If you do not, you will not be able to publish packages to the repository.

NOTE You do not need to run Package Studio as administrator if your repositories were configured on non-UAC protected paths or when you are running Package Studio and the repositories on machines other than a Windows 2008 Server.

Procedure

1. On a Windows 2008 machines, select **Start > All Programs > VMware vCenter Configuration Manager > Tools**.
2. Right-click **Package Studio** and select **Properties**.
3. Click the **Compatibility** tab.
4. In the Privilege Level area, select **Run this program as an administrator** and click **Apply**.
5. Click **OK**.
6. Select **Start > All Programs > VMware vCenter Configuration Manager > Tools > Package Studio**.
7. On the User Account Control dialog box, click **Yes**.

Using VCM Software Provisioning for Windows

Using VCM Software Provisioning, you collect and view Repository and Package Manager data, and then install or remove packages on target machines.

Prerequisites

Software packages are created and published to the repository. See "Creating Packages" on page 223.

Procedure

1. " Collect Package Manager Information from Machines" on page 226

   To view information about packages and Package Managers in VCM, you must collect Package Manager data from managed machines.

2. "Collect Software Repository Data" on page 226

   Collect the repository data to identify which software packages are in which repositories. From the collected information, you can determine which repositories to assign to machines based on the available packages.

3. "Add Repository Sources to Package Managers" on page 227

   Sources are the sections in the repository from which the Package Manager will be able to download and install packages.

4. "Install Packages" on page 228

   The process of installing packages includes identifying and processing dependencies and conflicts, running any specified prescripts, running the installation using any specified command arguments, and then running any specified post-scripts.

Collect Package Manager Information from Machines

To view information about packages and Package Managers in VCM, you must collect Package Manager data from managed machines.

As you work with provisioning, you will want to regularly collect Package Manager data to determine if your machines are remaining current with the necessary software packages.

Prerequisites

- Package Manager is installed on the target machines. Package Manager is automatically installed when you install the VCM 5.3 Agent or later. See "Install Package Manager on Managed Machines" on page 222.
- Verify that you created software provisioning packages using VMware vCenter Configuration Manager Package Studio and published the packages to the repositories. See "Creating Packages" on page 223.

Procedure

1. Click **Collect**.
2. Select **Machine Data**.
3. Click **OK**.
4. On the Machines page, verify that the **Selected** pane displays all the machines from which you are collecting package manager data and click **Next**.
5. On the Data Types page, expand **Windows**, select **Software Provisioning - Package Managers**, and click **Next**.
6. On the Confirmation page, review the information, resolve any conflicts, and then click **Finish**.

   You can monitor the process in the **Jobs Manager**. See "Viewing Provisioning Jobs in the Job Manager" on page 230 for more information.

What to do next

- When the collection is finished, view the collected data. Click **Console** and select **Windows tab > Operating System > Software Provisioning > Package Managers**. The data grid displays the packages and their current status.
- Collect repository data from the Software Repository for Windows. See "Collect Software Repository Data" on page 226.

Collect Software Repository Data

Collect the repository data to identify which software packages are in which repositories. From the collected information, you can determine which repositories to assign to machines based on the available packages.

To better manage your repository machines, create a machine group containing all the machines on which the software repository is installed.

Prerequisites

Verify that you created software provisioning packages using VMware vCenter Configuration Manager Package Studio and published the packages to the repositories. See "Creating Packages" on page 223.

Procedure

1. Click **Collect**.
2. Select **Machine Data**.
3. Click **OK**.
4. On the **Machines** page, verify that the **Selected** pane displays all the machines from which you are collecting repository data and click **Next**.
5. On the **Data Types** page, expand **Windows**, and select **Software Provisioning - Repositories**, and click **Next**.
6. On the Confirmation page, review the information, resolve any conflicts, and then click **Finish**.

   You can monitor the process in the **Jobs Manager**. See "Viewing Provisioning Jobs in the Job Manager" on page 230 for more information.

What to do next

- When the collection is finished, view the collected data. Click **Console** and select **Windows tab > Operating System > Software Provisioning > Repositories**. The data grid displays the packages in the repositories.
- Add the repositories to the Package Manager. See "Add Repository Sources to Package Managers" on page 227.

Add Repository Sources to Package Managers

Sources are the sections in the repository from which the Package Manager will be able to download and install packages.

Adding a source gives the Package Manager on the selected machines access to the packages available in specified section. The sources are numbered in priority order. When you add a new one, you can specify whether to add it to the beginning or to the end of the list. You can also remove sources.

Prerequisites

- Verify that you collected Package Manager data from the target machines. See " Collect Package Manager Information from Machines" on page 226.
- Verify that you collected repository data from software repository. See "Collect Software Repository Data" on page 226

Procedure

1. Click **Console**.
2. Select **Windows tab > Operating System > Software Provisioning > Package Managers**.
3. Select one or more machines, and then click **Add Source**.
4. On the Select Machines page, verify that the machines displayed in the lower pane are the machines to which you want to add the source and click **Next**.
5. On the Enter or Select Source page, configure the options and click **Next**.

a. Select either **Add source at the beginning of existing source lists** or **Add source at the end of the existing source list**.

b. Click **Browse Sources**.

c. On the **Browse Sources** page, select one of the following in the Show Sources from drop-down menu:

- **Package Manager Source Lists:** Select this option if you have already added sources to at least one Package Manager and you want to add the source to other Package Managers. When you click **OK**, the selected source automatically populates the **Platform** and **Section** field on the **Enter or Select Source** page.
- **VCM Managed Repositories:** Select this option if the source has not yet been added to a Package Manager. When you return to the **Enter or Select Source** page, you must type the platform and section names in the appropriate text boxes.

d. Select the URI and click **OK**.

e. Verify that the **Platform** name and the **Section** name exactly the names used in the repository.

6. On the Schedule page, select one of the scheduling options and configure as needed.
7. On the Confirmation page, review the information and click **Finish**.

   You can monitor the status of the process using **Jobs Manager > Running**.

The added source is displayed in the **Package Manager - Sources** data grid.

What to do next

Install software packages on target machines. See "Install Packages" on page 228.

Install Packages

The process of installing packages includes identifying and processing dependencies and conflicts, running any specified prescripts, running the installation using any specified command arguments, and then running any specified post-scripts. You can also remove packages.

Prerequisites

Verify that you added the repository sources to the Package Managers. See "Add Repository Sources to Package Managers" on page 227.

Procedure

1. Click **Console**.
2. Select **Windows tab > Operating System > Software Provisioning > Package Managers**
3. Click **Install Package**.
4. On the Select Machines page, verify that the machines displayed in the lower pane are the machines to which you want to install the package and click Next.
5. On the Select Package page, select the package to install.

6. Select one of the following version options.

Option	Description
Install Version	Installs the specified version. By default the operator equals the package selected in the list; however, you may select a different operator and type the version number in the text box.
Install latest available version on all platforms	Installs the latest version of the package available from the sources configured for the Package Manager.

7. Configure the Security Options and click **Next**.

   This option determines if a package is installed or removed based on the state of the signature. Select one of the following options.

Option	Description
Install secure signed package only	The package must be signed and the public key of the signing certificate you used to sign the package is available on all the machines on which you are installing or removing the package.
Skip signature validation when installing a signed package	(Not Recommended) The package is installed or removed without attempting to verify the signature.
Allow unsigned package to be installed	(Not recommended) The package is installed or removed even if it is unsigned.

8. On the Schedule page, select one of the scheduling options and configure as needed
9. On the Confirmation page, review the information, resolve any conflicts, and then click **Finish**.

   You can monitor the process in the **Jobs Manager**. See "Viewing Provisioning Jobs in the Job Manager" on page 230 for more information.

The package is displayed as Installed in the **Package Manager - Packages** data grid.

Related Software Provisioning Actions

You can use the following management options in VCM when working with software provisioning.

Option	Description
Console	All Software Provisioning are available for auditing as part of Change Management. Click Console and select **Change Management > VCM Initiated** or **Non VCM Initiated** to view the data. Software Provisioning actions are not eligible for rollback through Change Management. The undoing of any unwanted changes can be handled using Compliance enforcement remediation actions. See "Create Compliance Rules Containing Software Provisioning Remediation Actions" on page 232 for general information about remediation. Non VCM Initiated changes related to Software Provisioning include publishing packages to repositories from Package Studioand manually running command line actions in Package Manager.
Compliance	You can create compliance rules based on software provisioning data types, and you can add provisioning remediation actions to rules. See "Create Compliance Rules Based on Software Provisioning Data" on page 231 and "Create Compliance Rules Containing Software Provisioning Remediation Actions" on page 232.
Reports	You can run reports on collected Software Provisioning data. Click Reports and select **Machine Group Reports > Software Provisioning** to run the default reports, or you can create your own.
Administration	Displays current jobs running, and job history. Use the job history when troubleshooting the processing of a job. See "Viewing Provisioning Jobs in the Job Manager" on page 230 for more information. You can define user access rules and roles to specify what level of access users have to the Software Provisioning data and actions in VCM. Click Administration and select **User Rules and Roles > User Manager > VCM Access** to configure the Access Rules and Roles.

Viewing Provisioning Jobs in the Job Manager

The Jobs Manager tells you the state of a currently running Provisioning job, including the success or failure of a job, either collecting data from machines or installing, updating, or removing packages from machines.

The currently running provisioning jobs are visible in the following locations:

- Jobs button, located on the portal toolbar.
- Administration slider. Select **Administration > Job Manager > Running**.

Job history is available in **Administration > Job Manager > Other Jobs**. The provisioning related job names include the following:

- Change Request: Add Source
- Change Request: Remove Source
- Change Request: Install Package
- Change Request: Remove Package

Create Compliance Rules Based on Software Provisioning Data

A Compliance rule based on software provisioning data detects any packages or sources that are out of compliance. You can configure remediation actions to bring the machines back into compliance.

In this example the Compliance rule checks whether the source, where platform=Any and section=Release, was added to selected Package Managers as a source. If not, then add the repository source to the machines where the rule fails.

Procedure

1. Click **Compliance**.
2. Select **Machine Group Compliance > Rule Groups**.
3. Expand your rule group and select **Rules**.
4. On the Rules data grid, click **Add**.
5. Type a **Name** and **Description** for your rule and click **Next**.
6. On the Data Type page, expand **Windows** and select the data type on which you are basing the rule and click **Next**.

   The data type does not need to be software based. In this example, select **Services**.
7. On the Rule Type for Services page, select **Conditional (if/then)** and click **Next**.
8. On the Conditional Data page, configure the options.
   a. In the **IF** area, click **Add**.
   b. Select `Source Repository = YourRepository`.
   c. Select **Must Exist**.
   d. In the **THEN** area, select `Platform = Any` and `Section = Release`.
9. On the Options page, configure the settings.
   a. Select a **Severity** in the drop-down list.
   b. Select **Make available for enforcement where possible**.
   c. Select **Software Provisioning action**.
   d. Select **Add Source** in the drop-down list, and then click **Define Action**. The **Software Provisioning Compliance Remediation** page appears.
   e. Select **Add source to the beginning of existing source list**.
   f. Click **Browse Sources** to select the repository URI where the Platform=Any and Section=Release exist. The **Platform** and **Section** update with Any and Release respectively.
   g. Click **OK** to close the page.
   h. Click **Next**.
10. On the Collection filters page, select the **Provisioning - Package Managers** collection filter and click **Next**.
11. On the Important page, review the information and click **Finish** to save your rule.

When the Compliance Template is run, if the checks the target machines to determine if the repository source is added as a source. If it is not, the source is added to the machines Package Manager.

Create Compliance Rules Containing Software Provisioning Remediation Actions

When configuring a Compliance rule, you can configure the rule to perform a remediation based on a software provisioning action -- Install Package, Remove Package, Add Source, Remove Source.

In this example, you want to determine if a software application named XSoftware is correctly installed. If the software is installed correctly, a service named XService should be running. Configure a Compliance rule to determine if XService service is running. If it is not running, install the XSoftware package.

Procedure

1. Click **Compliance**.
2. Select **Machine Group Compliance > Rule Groups**.
3. Expand your rule group, and then select **Rules**.
4. On the Rules data grid, click **Add**.
5. On the Rule and Name page, type a **Name** and **Description** for your rule and click **Next**.
6. On the Data Type page, expand **Windows** and select the data type on which you are basing the rule and click **Next**.

   The data type does not need to be software based. In this example, select **Services**.
7. On the Rule Type for Services page, select **Conditional (if/then)** and click **Next**.
8. On the Conditional Data properties page, configure the options and click **Next**.
   a. In the **IF** section, click **Add**.
   b. Select `Services Name = XService`.
   c. Select **Must Exist**.
   d. In the **THEN** section, click **Add**.
   e. Select `State = Running`.
9. On the Options page, configure the options.
   a. Select a **Severity** in the drop-down list.
   b. Select **Make available for enforcement where possible**.
   c. Select **Software Provisioning action**.
   d. Select **Install Package** in the drop-down list, and then click **Define Action**. The **Software Provisioning Compliance Remediation** page appears.
   e. Select the `XSoftware` package to install if the rule you are configuring fails.

f. Configure the version options to use the selected version, specify a different version, or install the latest version.

g. Select one of the following **Security Options**:

This option determines if a package is installed or removed based on the state of the signature. Select one of the following options.

Option	Description
Install secure signed package only	The package must be signed and the public key of the signing certificate you used to sign the package is available on all the machines on which you are installing or removing the package.
Skip signature validation when installing a signed package	(Not Recommended) The package is installed or removed without attempting to verify the signature.
Allow unsigned package to be installed	(Not recommended) The package is installed or removed even if it is unsigned.

h. Click **OK** to close the page, and then click **Next**.

10. On the Collection filters page, select the `Services` collection filter and click **Next**.
11. On the Important page, review the information and click **Finish** to save your rule.

When the Compliance Template is run, if the check for XService running fails, the XSoftware package is installed.

Getting Started with VCM Management Extensions for Assets 13

VCM Management Extensions for Assets (VCMMXA) integrates and manages hardware and software asset data that is not gathered through the automated managed machine collection processes of VCM.

- **Hardware**. VCMMXA stores supplemental information (data that is not automatically collected) about physical and virtual machines that are managed by VCM. In addition, VCMMXA stores data about non-managed enterprise equipment such as printers, mobile devices, routers, and so on.
- **Software**. VCMMXA can collect and store information about the software that is installed on physical and virtual machines managed by VCM.

VCM users view the asset data in the VCM Console, where, depending on assigned role, users may also have edit permission.

Configure Asset Data Fields

An administrator must configure VCMMXA so that it includes the columns of data that apply to the hardware and software assets in your environment.

Procedure

1. "Review Available Asset Data Fields" on page 236

   VCMMXA is prepopulated with a short list of data fields to get you started.

2. "Add an Asset Data Field" on page 236

   You can add any data that you want to store and manage about your hardware or software.

3. "Edit an Asset Data Field" on page 237

   Change VCMMXA asset data fields to keep up with your tracking and management needs for hardware or software.

4. "Delete a VCMMXA Data Field" on page 238

   Remove asset data fields that do not serve a purpose in your environment.

5. "Change the Order of Asset Data Columns" on page 238

   Changing the order of the VCMMXA asset data field list changes the order of columns when you view asset data in the VCM Console.

6. "Refresh Dynamic Asset Data Fields" on page 239

   You can force VCMMXA to refresh the values in all fields that are configured to populate dynamically.

Review Available Asset Data Fields

VCMMXA is prepopulated with a short list of data fields to get you started. Examples include hardware data such as location or contact person, and software data such as license expiration date or number of copies.

VCMMXA is configurable, however, so review the data fields and the order in which they appear. You have the opportunity to add, modify, remove, and rearrange fields to suit your needs.

Prerequisites

- Log in to VCM using an account with the Administrator role.
- Identify what asset data you want to store about your hardware or software.

Procedure

1. Click **Administration**.
2. Select **Settings > Asset Extensions Settings**.
3. Select one of the following.

   Hardware Configuration Items > Other Devices
   Hardware Configuration Items > VCM Devices
   Software Configuration Items
4. In the data grid, review the names and descriptions.

   Each row, in order, becomes a column in the asset data display in the VCM Console.

What to do next

Supplement the prepopulated fields by adding more fields. See "Add an Asset Data Field" on page 236.

Add an Asset Data Field

You can add any data that you want to store and manage about your hardware or software.

Prerequisites

- Log in to VCM using an account with the Administrator role.
- Identify what asset data you want to store about your hardware or software.

Procedure

1. Click **Administration**.
2. Select **Settings > Asset Extensions Settings**.
3. Select one of the following.

   Hardware Configuration Items > Other Devices
   Hardware Configuration Items > VCM Devices
   Software Configuration Items
4. Click **Add**.
5. Type a name and description for the new asset data field and click **Next**.

   The name is the column heading that appears when users view the data in the VCM Console.
6. Specify properties about the new data.

a. Select the way to populate the data.

Manually—type free-form text
Lookup—select from a fixed or query-based list of values
Dynamically—query from other data

b. Select the data type.

For string data, also enter the maximum number of characters to allow.

7. Click **Next**.
8. (Lookup, fixed) Create the fixed list by typing values and clicking **Add**.
9. (Lookup, query-based) Type the SQL query that populates the list from which to select values.
10. (Dynamic) Type the SQL query that pulls the value from another data source.
11. (Lookup or dynamic) Click **Next**.
12. (All) Select the roles that are allowed to edit the data.

    Only users assigned to these roles will be able to edit the data using the VCM Console.
13. Review the settings and click **Finish**.

What to do next

Modify fields that need to be adapted for your site. See "Edit an Asset Data Field" on page 237.

Edit an Asset Data Field

Change VCMMXA asset data fields to keep up with your tracking and management needs for hardware or software.

Prerequisites

- Log in to VCM using an account with the Administrator role.
- Identify what asset data you want to store about your hardware or software.

Procedure

1. Click **Administration**.
2. Select **Settings > Asset Extensions Settings**.
3. Select one of the following.

   Hardware Configuration Items > Other Devices
   Hardware Configuration Items > VCM Devices
   Software Configuration Items
4. In the data grid, select the row.
5. Click **Edit**.
6. Change the name or description for the field and click **Next**.

   The name is the column heading that appears when users view the data in the VCM Console.
7. Click **Next**.

When editing, you cannot change the data properties.

8. Click **Next**.
9. Select the roles that are allowed to edit the data.

   Only users assigned to these roles will be able to edit the data using the VCM Console.
10. Review the settings and click **Finish**.

What to do next

Remove unwanted fields. See "Delete a VCMMXA Data Field" on page 238.

Delete a VCMMXA Data Field

Remove asset data fields that do not serve a purpose in your environment.

Prerequisites

- Log in to VCM using an account with the Administrator role.
- Identify what asset data you want to store about your hardware or software.

Procedure

1. Click **Administration**.
2. Select **Settings > Asset Extensions Settings**.
3. Select one of the following.

   Hardware Configuration Items > Other Devices
   Hardware Configuration Items > VCM Devices
   Software Configuration Items
4. In the data grid, select the row.
5. Click **Delete**.

   You cannot delete entries that are marked with a lock icon.
6. Click **OK**.

What to do next

Rearrange asset data fields so that the order of columns shown in the VCM Console meets your requirements. See "Change the Order of Asset Data Columns" on page 238.

Change the Order of Asset Data Columns

Changing the order of the VCMMXA asset data field list changes the order of columns when you view asset data in the VCM Console.

Prerequisites

- Log in to VCM using an account with the Administrator role.
- Identify what asset data you want to store about your hardware or software.

Procedure

1. Click **Administration**.
2. Select **Settings > Asset Extensions Settings**.
3. Select one of the following.

   Hardware Configuration Items > Other Devices
   Hardware Configuration Items > VCM Devices
   Software Configuration Items

   In the data grid, each row, in order, becomes a column in the asset data display in the VCM Console.
4. Click **Column Order**.
5. Select entries, use the arrow buttons to move rows up or down, and click **Next**.
6. Review the rearranged order and click **Finish**.

What to do next

Refresh the values in dynamically generated fields. See "Refresh Dynamic Asset Data Fields" on page 239.

Refresh Dynamic Asset Data Fields

You can force VCMMXA to refresh the values in all fields that are configured to populate dynamically.

Prerequisites

Log in to VCM using an account with the Administrator role.

Procedure

1. Click **Administration**.
2. Select **Settings > Asset Extensions Settings**.
3. Select one of the following.

   Hardware Configuration Items > Other Devices
   Hardware Configuration Items > VCM Devices
   Software Configuration Items
4. Click **Refresh Dynamic Fields**.

   The option recalculates and overwrites all dynamic data fields listed and may take time to complete.
5. Click **OK**.

What to do next

Enter data for machines that are managed by VCM. See "Configure Asset Data Values for VCM Machines" on page 239.

Configure Asset Data Values for VCM Machines

Although the asset data for machines that are managed by VCM is automatically collected, you can customize some data through VCMMXA.

Prerequisites

Log in to VCM with a role that has edit permission for asset configuration data.

Procedure

1. Click **Console**.
2. Select **Asset Extensions > Hardware Configuration Items > VCM Devices**.
3. In the data grid, select the VCM machine.
4. Click **Edit Values**.
5. Verify that the machine you want is in the Selected list and click **Next**.

   Use the arrow buttons to move entries to or from the Selected list.
6. Move the data fields that you want to edit into the Selected list and click **Next**.

   Use the arrow buttons to move entries to or from the Selected list.
7. Select or type the new values and click **Next**.
8. Review the new values and click **Finish**.

What to do next

Enter data for hardware that is not managed by VCM, such as printers, mobile devices, routers, and so on. See "Configure Asset Data for Other Hardware Devices" on page 240.

Configure Asset Data for Other Hardware Devices

A user with a role that has permission to edit asset data can populate VCMMXA with the hardware devices in your environment that are not automatically discovered and managed by VCM.

Procedure

- "Add Other Hardware Devices" on page 240

  Use VCMMXA to keep track of your non VCM managed hardware by adding information about the hardware devices directly to VCM.
- "Add Multiple Similar Other Hardware Devices" on page 241

  If your site has many nearly identical devices, you can use VCMMXA to clone one copy as a way to quickly add records for the other devices.
- "Edit Asset Data for Other Hardware Devices" on page 241

  Use VCMMXA to change your hardware asset records as your enterprise changes.
- "Edit Asset Data Values for Other Hardware Devices" on page 242

  You can change only the details about a given piece of equipment when the long term information, such as the model name or number, is going to remain the same.
- "Delete Other Hardware Devices" on page 242

  Use VCMMXA to delete the records of hardware devices that are no longer a part of your site.

Add Other Hardware Devices

Use VCMMXA to keep track of your non VCM managed hardware by adding information about the hardware devices directly to VCM.

Prerequisites

- Have an administrator configure the asset data fields that you need. See "Configure Asset Data Fields" on page 235.
- Log in to VCM with a role that has edit permission for asset configuration data.

Procedure

1. Click **Console**.
2. Select **Asset Extensions > Hardware Configuration Items > Other Devices**.
3. Click **Add**.
4. Select or type the details that identify the device, such as its name and model, and click **Next**.
5. Select or type the values for the asset data associated with the device and click **Next**.

   The fields can vary depending on how the administrator configured your data for other hardware devices.
6. Click **Finish**.

Add Multiple Similar Other Hardware Devices

If your site has many nearly identical devices, you can use VCMMXA to clone one copy as a way to quickly add records for the other devices.

Prerequisites

- Log in to VCM with a role that has edit permission for asset configuration data.
- Create at least one copy of the device to serve as a baseline. See "Add Other Hardware Devices" on page 240.

Procedure

1. Click **Console**.
2. Select **Asset Extensions > Hardware Configuration Items > Other Devices**.
3. In the data grid, select the original, baseline asset.
4. Click **Clone**.
5. Modify the details to reflect the new copy of the asset and click **Next**.

   You must change at least the name.
6. Modify the values to reflect the asset data associated with the new device and click **Next**.
7. Click **Finish**.

Edit Asset Data for Other Hardware Devices

Use VCMMXA to change your hardware asset records as your enterprise changes.

Prerequisites

Log in to VCM with a role that has edit permission for asset configuration data.

Procedure

1. Click **Console**.
2. Select **Asset Extensions > Hardware Configuration Items > Other Devices**.
3. In the data grid, select the asset.
4. Click **Edit**.
5. Change the details that identify the device, such as its name and model, and click **Next**.
6. Change the values for the asset data associated with the device and click **Next**.

   The fields can vary depending on how the administrator configured your data for other hardware devices.
7. Click **Finish**.

Edit Asset Data Values for Other Hardware Devices

You can change only the details about a given piece of equipment when the long term information, such as the model name or number, is going to remain the same.

Prerequisites

Log in to VCM with a role that has edit permission for asset configuration data.

Procedure

1. Click **Console**.
2. Select **Asset Extensions > Hardware Configuration Items > Other Devices**.
3. In the data grid, select the asset.
4. Click **Edit Values**.
5. Move the data fields that you want to edit into the Selected list and click **Next**.

   Use the arrow buttons to move entries to or from the Selected list.
6. Select or type the new values and click **Next**.
7. Review the new values and click **Finish**.

Delete Other Hardware Devices

Use VCMMXA to delete the records of hardware devices that are no longer a part of your site.

Prerequisites

Log in to VCM with a role that has edit permission for asset configuration data.

Procedure

1. Click **Console**.
2. Select **Asset Extensions > Hardware Configuration Items > Other Devices**.
3. In the data grid, select the asset.
4. Click **Delete**.
5. Click **OK**.

Configure Asset Data for Software

A user with a role that has permission to edit asset data can use VCMMXA to gather information about the software on machines that are discovered and managed by VCM.

Procedure

- "Add Software Assets" on page 243

  Manage your software assets by having VCMMXA detect what is installed on the physical and virtual machines in your environment.

- "Add Multiple Similar Software Assets" on page 244

  If your environment has many nearly identical copies of software, such as the same application with a different license number, you can use VCMMXA to clone one copy as a way to quickly add records for the others.

- "Edit Asset Data for Software" on page 245

  Use VCMMXA to change your software asset records as your enterprise changes.

- "Edit Asset Data Values for Software" on page 245

  You can change the details about a specific copy of software when the long term information, such as the application name or version, is going to remain the same.

- "Delete Software Data" on page 246

  xUse VCMMXA to delete entries for software that is no longer installed at your site.

Add Software Assets

Manage your software assets by having VCMMXA detect what is installed on the physical and virtual machines in your environment.

Prerequisites

- Have an administrator configure the asset data fields that you need. See "Configure Asset Data Fields" on page 235.
- Log in to VCM with a role that has edit permission for asset configuration data.

Procedure

1. Click **Console**.
2. Select **Asset Extensions > Software Configuration Items**.
3. Click **Add Software**.
4. Type a name and description and click **Next**.
5. Select what data type VCMMXA will look for in order to detect the installed software and click **Next**.

   The options take you to custom wizard pages where you type or select what VCMMXA will look for in the database.

- **Software Inventory (Windows)**—Select a product from the software inventory (SI) list.
- **Registry (Windows)**—Type or select a Windows Registry path, key, and value.
- **File System - Known Files (Windows)**—Type or select a filename and version.
- **Software Inventory - Packages (UNIX)**—Select a product from the SI list.
- **Software Inventory - Utilities (UNIX)**—Select a product from the SI list.
- **File System - Known Files (UNIX)**—Type or select a filename.

6. Click **Next**.
7. Select or type the values for the asset data associated with the software and click **Next**.

   The fields can vary depending on how the administrator configured your data for software.
8. Click **Finish**.

Add Multiple Similar Software Assets

If your environment has many nearly identical copies of software, such as the same application with a different license number, you can use VCMMXA to clone one copy as a way to quickly add records for the others.

Prerequisites

- Log in to VCM with a role that has edit permission for asset configuration data.
- Create at least one copy of the software to serve as a baseline. See "Add Software Assets" on page 243.

Procedure

1. Click **Console**.
2. Select **Asset Extensions > Software Configuration Items**.
3. In the data grid, select the original, baseline software asset.
4. Click **Clone**.
5. Modify the details to reflect the new copy of the software asset and click **Next**.

   You must change at least the name.
6. Change what data type VCMMXA will look for in order to detect the installed software and click **Next**.

   The options take you to custom wizard pages where you type or select what VCMMXA will look for in the database.

   - **Software Inventory (Windows)**—Select a product from the software inventory (SI) list.
   - **Registry (Windows)**—Type or select a Windows Registry path, key, and value.
   - **File System - Known Files (Windows)**—Type or select a filename and version.
   - **Software Inventory - Packages (UNIX)**—Select a product from the SI list.
   - **Software Inventory - Utilities (UNIX)**—Select a product from the SI list.
   - **File System - Known Files (UNIX)**—Type or select a filename.
7. Click **Next**.
8. Modify the asset data values to reflect the new software and click **Next**.
9. Click **Finish**.

Edit Asset Data for Software

Use VCMMXA to change your software asset records as your enterprise changes.

Prerequisites

Log in to VCM with a role that has edit permission for asset configuration data.

Procedure

1. Click **Console**.
2. Select **Asset Extensions > Software Configuration Items**.
3. In the data grid, select the software asset.
4. Click **Edit**.
5. Change the name or description and click **Next**.
6. Change what data type VCMMXA will look for in order to detect the installed software and click **Next**.

   The options take you to custom wizard pages where you type or select what VCMMXA will look for in the database.

   - **Software Inventory (Windows)**—Select a product from the software inventory (SI) list.
   - **Registry (Windows)**—Type or select a Windows Registry path, key, and value.
   - **File System - Known Files (Windows)**—Type or select a filename and version.
   - **Software Inventory - Packages (UNIX)**—Select a product from the SI list.
   - **Software Inventory - Utilities (UNIX)**—Select a product from the SI list.
   - **File System - Known Files (UNIX)**—Type or select a filename.
7. Click **Next**.
8. Change the values for the asset data associated with the software and click **Next**.

   The fields can vary depending on how the administrator configured your data for software.
9. Click **Finish**.

Edit Asset Data Values for Software

You can change the details about a specific copy of software when the long term information, such as the application name or version, is going to remain the same.

Prerequisites

Log in to VCM with a role that has edit permission for asset configuration data.

Procedure

1. Click **Console**.
2. Select **Asset Extensions > Software Configuration Items**.
3. In the data grid, select the software asset.
4. Click **Edit Values**.
5. Move the data fields that you want to edit into the Selected list and click **Next**.

   Use the arrow buttons to move entries to or from the Selected list.
6. Select or type the new values and click **Next**.
7. Review the new values and click **Finish**.

Delete Software Data

Use VCMMXA to delete entries for software that is no longer installed at your site.

Prerequisites

Log in to VCM with a role that has edit permission for asset configuration data.

Procedure

1. Click **Console**.
2. Select **Asset Extensions > Software Configuration Items**.
3. In the data grid, select the software asset.
4. Click **Delete**.
5. Click **OK**.

Getting Started with VCM Service Desk Integration

14

VCM Service Desk Integration tracks planned and unplanned changes to managed machines in your organization, and integrates change requests with your change management process.

Service Desk Integration works by temporarily holding requested changes to managed machines while VCM integrates with your service desk application in order to pass the requests through your change management process or workflow. After the changes are approved, VCM resumes changing the managed machines, in order of criticality.

VCM Service Desk Connector links VCM with the service desk application in order to track and manage the VCM initiated changes. Change management process and workflow definitions vary by customer and depend on the configuration implemented during your VMware services engagement.

Configure Service Desk Integration

To add the Service Desk Integration feature to VCM, you must complete the following high-level tasks.

Procedure

1. Contact VMware Customer Support to determine the requirements for your integration and arrange for a VMware services engagement.
2. License Service Desk Integration.
3. Activate Service Desk Integration

After VMware Customer Support assists you with licensing and the integration of VCM with your service desk application, additional nodes that are unique to the service desk feature appear in VCM.

What to do next

Look at your service desk data. See "View Service Desk Integration in the Console" on page 247.

View Service Desk Integration in the Console

When service desk integration is enabled, the Service Desk data grids provide a detailed view of VCM-related service desk events.

Procedure

1. Click **Console**.
2. Select **Service Desk**.
3. Under the Service Desk node, select any sub-node.

   For example, click **By RFC** to view the data according to request for change (RFC). Under the By RFC sub-node, select an RFC to view the data for that item.

Be aware the your sub-nodes and data views may differ from the defaults or from other organizations based on your requirements and specific implementation.

What to do next

Look at the status of change jobs. See "View Service Desk Integration in Job Manager" on page 248.

View Service Desk Integration in Job Manager

VCM Service Desk Integration pauses requested changes to managed machines while VCM integrates with your service desk application to pass the request through your change management process.

Procedure

1. Click **Administration**.
2. Select **Job Manager > Pending Response**.

   After the job is approved, it is released to run immediately or at a scheduled time.
3. Select **Job Manager > Running**.

   Alternately, select **Job Manager > Scheduled**.

NOTE Locate patching jobs by clicking **Patching** and selecting **VCM Patching Administration > *{operating-system}* > Job Manager**.

Getting Started with VCM for Active Directory 15

VCM for Active Directory collects Active Directory objects across domains and forests, and displays them through a single console. The information is consolidated and organized under the Active Directory slider, allowing you to view your Active Directory structure, troubleshoot issues, detect change, and ensure compliance.

You can filter, sort, and group Active Directory data to pinpoint the specific area of interest. You can also view a subset of your Active Directory (a forest, domain, or specific organizational unit branch) by setting the Active Directory location in the AD Location field near the top of VCM. Dashboards display high level information in graphical form, alerts notify you about problems or misconfigurations, and change management tracks changes to the Active Directory objects or configuration by data type.

Configure Domain Controllers

To manage your Active Directory environment, you must verify domains and accounts, discover and license domain controllers, install the VCM Agent, and collect data from the domain controllers.

Procedure

1. "Verify Available Domains" on page 250

   Allow VCM access to each domain so that the VCM Collector can interact with the domain controllers in your environment.

2. "Check the Network Authority Account" on page 250

   Verify that at least one domain account with administrator privileges is available to act as a network authority account for VCM.

3. "Assign Network Authority Accounts" on page 251

   Select and assign the network authority account that you identified for VCM access to the domain controllers.

4. "Discover Domain Controllers" on page 251

   Identify the domain controllers in your network that you are managing with VCM.

5. "License Domain Controllers" on page 252

   To manage domain controllers, you must license them in VCM.

6. "Install the VCM Windows Agent on Your Domain Controllers" on page 253

   Install the VCM Windows Agent on each domain controller to manage.

7. Collect Domain Controller Data

   Start managing the domain controllers by performing an initial collection, which adds domain controller data to VCM.

Continuous domain controller management is based on the latest data that you collect from target machines. You can view data and run actions, such as reports or compliance, based on the collected data. See "Windows Collection Results" on page 91.

Verify Available Domains

Allow VCM access to each domain so that the VCM Collector can interact with the domain controllers in your environment.

During installation, VCM discovered all domains to which the network authority account had access. If the domain controllers belong to a domain that is not listed, you must add that domain manually.

Prerequisites

Know the fully-qualified names of the domains to manage.

Procedure

1. Click **Administration**.
2. Select **Settings > Network Authority > Available Domains**.
3. Verify that the domain appears in the Available Domains view and has a **Domain Type** of Active Directory.
4. If the domain does not appear, add the domain.
   a. Click **Add**.
   b. Type the domain name and select the domain type as **AD**, and click **OK**.

What to do next

Verify that a network authority account is available and create other necessary domain accounts. See "Check the Network Authority Account" on page 250.

Check the Network Authority Account

Verify that at least one domain account with administrator privileges is available to act as a network authority account for VCM.

VCM network authority accounts must have administrator privileges on each domain to be managed in the organization. Although you specified an initial default network authority account when you installed VCM, you can add different administrator accounts if you do not assign the default account.

Prerequisites

Verify the presence of domains. See "Verify Available Domains" on page 250.

Procedure

1. Click **Administration**.
2. Select **Settings > Network Authority > Available Accounts**.
3. To add a new domain account, click **Add**.
4. Type the domain name, user name, and password, and click **Next**.
5. Click **Finish** to add the account.

What to do next

Assign the network authority account to the domain so that VCM can access the domain controllers in the domain. See "Assign Network Authority Accounts" on page 251.

Assign Network Authority Accounts

Select and assign the network authority account that you identified for VCM access to the domain controllers.

Assign an account with administrator privileges on the domain.

Prerequisites

Verify or add the necessary network authority account. See "Check the Network Authority Account" on page 250.

Procedure

NOTE You must perform these steps twice, once for NetBios and once for Active Directory.

1. Click **Administration**.
2. Select **Settings > Network Authority > Assigned Accounts > By Domain > NetBios**.
3. Select an assigned account.
4. Click **Edit Assigned Accounts**.
5. Select the account to receive authority to the domain and click **Next**.
6. Confirm the accounts to include in the authority list for the domain and click **Finish**.

What to do next

- Repeat the preceding assignment steps, and select Active Directory in step 2.
- Discover the domain controllers in your environment. See "Discover Domain Controllers" on page 251.

Discover Domain Controllers

Identify the domain controllers in your network that you are managing with VCM.

To discover the available domain controllers, VCM uses general discovery rules to identify many Windows machines or specific discovery rules to identify particular Windows machines.

The time required to perform an initial discovery depends on the size and composition of your network. If all domain controllers are not available during initial discovery, such as systems that are disconnected from the network, the first discovery will not find all domain controllers. If the discovery does not identify all domain controllers, you might need to run additional discoveries after the other domain controllers become available.

NOTE The Discovered Machines Import Tool (DMIT) can import many physical and virtual machines at one time into the VCM database. The tool imports machines discovered by the Network Mapper (Nmap). Download DMIT from the VMware Web site.

Prerequisites

Assign a Network Authority Account that VCM can use for access. See "Assign Network Authority Accounts" on page 251.

Procedure

1. Click **Administration**.
2. Select **Machines Manager > Discovery Rules**.
3. Click **Add** to create a discovery rule.
4. Type a name and description and click **Next**.
5. Select **By Browse List** and click **Next**.
6. Select **Only discover machines in the Browse List that match these criteria**.
7. Select and type the following filter parameters.

   Where **Domain Controller Type** **< >** " (two single quotes, no space)
8. Click **Next**.
9. Click **Yes** and **Finish**.
10. On the toolbar, click **Jobs** to track current discovery job status.

    The Jobs Running window displays the job name and summary information while the job runs.

What to do next

- Verify that jobs have finished running. Click **Administration** and select **Job Manager > History > Other Jobs > Past 24 Hours**.
- Verify that the domain controllers are available. Click **Administration** and select **Machines Manager > Available Machines > Available Windows Machines**.
- License the domain controllers in your environment. See "License Domain Controllers" on page 252.

License Domain Controllers

To manage domain controllers, you must license them in VCM.

The number of discovered domain controllers might exceed the number of your available licenses. If that happens, a message appears indicating that not enough licenses are available.

Prerequisites

Verify that the domain controllers you are licensing are listed with a machine type of workstation or server in **Available Windows Machines** in the following procedure. If the type is not workstation or server, VCM cannot license the machines. Contact VMware Technical Support to resolve a machine type that is not recognized by VCM.

Procedure

1. Click **Administration**.
2. Select **Machines Manager > Available Machines > Available Windows Machines**.
3. Select the domain controllers to license.
4. Click **License**.
5. Verify that the domain controllers to license appear in the Selected list.

   Use the arrows to move the domain controllers.

   Do not select the **Install VCM Agents for the selected machines** check box.
6. Click **Next** to view your Product License Details.

   The licensed domain controller count increases by the number of licensed machines.
7. Click **Next**.

   VCM confirms that the licenses you requested will be applied to the selected domain controllers.
8. Click **Finish**.

What to do next

- If you are working with Windows 7, 2008, 2008 R2, or Vista domain controllers, disable User Account Control (UAC). See the instructions in "Disable User Account Control for VCM Agent Installation" on page 81 before you proceed.
- Install the VCM Windows Agent. See "Install the VCM Windows Agent on Your Domain Controllers" on page 253.

Install the VCM Windows Agent on Your Domain Controllers

Install the VCM Windows Agent on each domain controller to manage.

Before you can collect data from domain controllers, you must install the VCM Windows Agent on the licensed domain controllers in your environment to enable communication between the Collector and the target machines.

Prerequisites

- License the domain controllers on which you install the Agent. See "License Domain Controllers" on page 252.
- Disable UAC before you install the Agent on Windows 7, 2008, 2008 R2, or Vista machines. See "Disable User Account Control for VCM Agent Installation" on page 81.

Procedure

1. Click **Administration**.
2. Select **Machines Manager > Licensed Machines > Licensed Windows Machines**.
3. In the data grid, select one or more domain controllers on which to install the Agent and click **Install**.

4. On the Machines page, verify that the target machines appear in the Selected list and click **Next**.
5. On the Install Options page, select the default installation options and click **Next**.
6. On the Schedule page, select **Run Action now** and click **Next**.

   You can schedule subsequent Agent installations to run later.
7. Review the summary information and click **Finish**.

What to do next

- Verify that jobs have finished running. Click **Administration** and select **Job Manager > History > Other Jobs > Past 24 Hours**.
- If you are working with Windows 7, 2008, 2008 R2, or Vista domain controllers, enable User Account Control (UAC). See the instructions in "Enable UAC After VCM Agent Installation" on page 89 before you proceed.
- Collect Windows data from VCM managed domain controllers in your environment. See "Collect Domain Controller Data" on page 254.

Collect Domain Controller Data

Start managing the domain controllers by performing an initial collection, which adds domain controller data to VCM.

Use the default filter set to collect a general view of the domain controllers in your environment. The first time that you use the default filter to collect data, the Windows Agent returns all of the data specified in the filter and stores the data in the VCM database. All subsequent collections will return a delta against the data previously collected.

A delta collection includes only the differences between the data on the target machine and the data stored in the VCM database. If you need a full collection, you can specify that VCM collect all data again. A full collection can take a significant amount of time depending on the number of VCM managed domain controllers from which you are collecting.

When you perform a full collection from your entire environment, run the collection during non working hours so that users do not notice any performance impact on managed machines. After the initial collection is finished, subsequent delta collections will most likely not impact performance.

Prerequisites

- To collect from Windows XP SP2 or Vista machines that use DCOM communication, you must enable ICMP pings in the firewall settings or disable ICMP pings in VCM.
- Verify that DCOM is enabled on the managed machine. Run `dcomcnfg` and select **Enable Distributed COM on this computer**.

Procedure

1. On the VCM toolbar, click **Collect**.
2. On the Collection Type page, select **Machine Data** and click **OK**.
3. On the Machines page, select the domain controllers from which to collect data and click **Next**.

   To move all visible domain controllers to the selection window, use the double arrow.
4. Select the **Do not limit collection to deltas** check box.

This option ensures that a full collection occurs during the initial set up of VCM for Active Directory.

5. On the Data Types page, select **Machines**.
6. Select **Use default filters** and click **Next**.
7. On the Important page, resolve any conflicts and click **Finish**.

What to do next

Add VCM for Active Directory. See "Configure VCM for Active Directory as an Additional Product" on page 255.

Configure VCM for Active Directory as an Additional Product

After VCM has discovered, licensed, and installed the Windows Agent on your domain controllers, configure VCM for Active Directory as an additional product. Configuring VCM for Active Directory provides the mechanism that allows VCM to manage the Active Directory forests and collect detailed schema information.

Procedure

1. "Install VCM for Active Directory on the Domain Controllers" on page 255

   To use VCM to collect Active Directory data from your environment, install VCM for Active Directory on your domain controllers.

2. "Run the Determine Forest Action" on page 256

   VCM for Active Directory requires a forest determination for all domain controllers so that it can proceed with schema and structure collection.

3. "Run the Domain Controller Setup Action" on page 256

   VCM for Active Directory collects your Active Directory schema and structure as part of the domain controller setup action.

Install VCM for Active Directory on the Domain Controllers

To use VCM to collect Active Directory data from your environment, install VCM for Active Directory on your domain controllers.

VCM for Active Directory will operate with only a single domain controller configured with VCM for Active Directory, which will serve as both the forest data source (FDS) and replication data source (RDS). However, to collect important non replicated attributes such as Last Logon, install VCM for Active Directory on as many domain controllers as possible.

Prerequisites

- Discover, license, and install the VCM Windows Agent on your domain controllers. See "Configure Domain Controllers" on page 249.
- Verify that jobs have finished running. Click **Administration** and select **Job Manager > History > Other Jobs > Past 24 Hours**.

Procedure

1. Click **Administration**.
2. Select **Machines Manager > Additional Components > VCM for Active Directory**.
3. Click **Install**.
4. Move the domain controllers on which to install VCM for Active Directory to the lower pane.
5. Click **Next**.
6. Verify that **Run Action now** is selected and click **Finish**.

If you add future Active Directory machines to your environment, configure them with VCM for Active Directory by running the following installer.

```
Program Files (x86)\VMware\VCM\AgentFiles\ADProductInstall.exe
```

What to do next

Determine the Active Directory forest in your environment. See "Run the Determine Forest Action" on page 256.

Run the Determine Forest Action

VCM for Active Directory requires a forest determination for all domain controllers so that it can proceed with schema and structure collection.

Prerequisites

- Install VCM for Active Directory on your domain controllers. See "Install VCM for Active Directory on the Domain Controllers" on page 255.
- Verify that jobs have finished running. Click **Administration** and select **Job Manager > History > Other Jobs > Past 24 Hours**.

Procedure

1. Click **Administration**.
2. Select **Machines Manager > Additional Components > VCM for Active Directory**.
3. Click **Determine Forest**.
4. Move the domain controllers on which to determine the forest to the lower pane.

   Determine the forest for all available domain controllers.
5. Click **Next**.
6. Click **Finish**.

What to do next

Run the domain controller setup action and identify your FDS and RDS. See "Run the Domain Controller Setup Action" on page 256.

Run the Domain Controller Setup Action

VCM for Active Directory collects your Active Directory schema and structure as part of the domain controller setup action.

During setup, you select a Forest Data Source (FDS) and Replication Data Source (RDS). Select machines that have reliable connections and availability. The same domain controller is allowed to serve as both FDS and RDS.

- **FDS**. VCM for Active Directory uses the FDS as a resource for all Forest-level information. You identify one FDS for each Forest.
- **RDS**. The RDS supplies all replicated data to VCM for Active Directory. You identify only one RDS for each domain so that collections on replicated attributes are performed only on a single domain controller. Other domain controllers that have VCM for Active Directory installed will be accessed only during collection of non replicated attributes.

  If you change your RDS, VCM for Active Directory does not purge data collected from the old RDS. Instead, the data is refreshed when you run a new collection using the new RDS.

Prerequisites

- Use VCM for Active Directory to determine the Forest. See "Run the Determine Forest Action" on page 256.
- Verify that jobs have finished running. Click **Administration** and select **Job Manager > History > Other Jobs > Past 24 Hours**.

Procedure

1. Click **Administration**.
2. Select **Machines Manager > Additional Components > VCM for Active Directory**.
3. Click **Setup DCs**.
4. Select an FDS for each forest and click **Next**.
5. Select an RDS for each domain and click **Next**.
6. Click **Finish**.

When the Setup DCs action finishes, VCM for Active Directory initiates the following jobs.

- Active Directory schema collection
- Active Directory specifier collection
- Active Directory structure collection

The information obtained from the third collection identifies the organizational unit (OU) structure that supports the use of VCM for Active Directory. To view information, click **Administration**, and select **Machines Manager > Additional Components > VCM for Active Directory**.

What to do next

Collect Active Directory data. See "Collect Active Directory Data " on page 257.

Collect Active Directory Data

Perform your first collection of Active Directory objects by launching the same collection wizard that you use for Windows and UNIX/Linux collections. The first time you run an Active Directory collection, the Agent returns all objects and attributes from your selected Active Directory environment.

Prerequisites

- Install VCM for Active Directory. See "Configure VCM for Active Directory as an Additional Product" on page 255.
- Verify that jobs have finished by clicking **Administration** and selecting **Job Manager > History > Other Jobs > Past 24 Hours**.

Procedure

1. From the toolbar, click **Collect**.
2. On the Collection Type page, select **Active Directory** and click **OK**.
3. On the AD Collection Options page, click **Select Data Types to collect from these machines**.
4. To ensure that a full collection occurs, select the **Do not limit collection to deltas** check box and click **Next**.
5. On the Data Types page, click **Select All**.
6. Select the **Use default filters** option and click **Next**.
7. On the Location page, click the ellipsis button (...).
8. On the Select an AD Location page, expand the **Enterprise** tree, select an Active Directory Location, and click **OK**.
9. On the Location page, click **Next**.
10. Click **Finish**.

What to do next

Explore initial Active Directory collection results. See "Active Directory Collection Results" on page 258.

Active Directory Collection Results

After you collect the initial Active Directory data, explore the results under Active Directory, Reports, and Compliance.

Displayed information is only as current as the last time that you collected Active Directory data.

Option	Description
Active Directory Dashboard	Provides summary and day-to-day information about your Active Directory environment in a graphical format. ■ To view the dashboard, click **Active Directory** and select **Dashboards > Managed Objects**. Several Active Directory Dashboards are available.
Active Directory Object Summary	Provides summary information about your Active Directory environment in a textual format. ■ To view the summary reports, click **Active Directory** and select **Objects > *object-type***.
Active Directory Object Detail	Provides the detailed information behind the summary for your Active Directory environment. ■ To view the detailed information, click **Active Directory** and select **Objects > *object-type***. Click the **View data grid** button. From the data grid view, you can enable or disable the summary to view the details immediately.
Reports	Provides Active Directory information by running pre-configured or custom reports against the latest collected data. The time needed for a report to generate depends on the volume or complexity of the data

Option	Description
	requested. ■ To use the reporting options, click **Reports** and expand **Active Directory Reports**.
Compliance	Provides preconfigured Active Directory compliance rules and templates, which allow you to check the collected data against specific values. ■ To view Active Directory compliance rules, click **Compliance** and select **Active Directory Compliance > Rule Groups**. ■ To view Active Directory compliance templates, click **Compliance** and select **Active Directory Compliance > Templates**.

Installing and Getting Started with VCM Tools

16

VCM Installation Manager installs several VCM components and tools on the Collector machine during the installation.

Using VCM Installation Manager, you can install the following tools.

- "Run the Import/Export Tool" on page 263

  Use the Import/Export Tool to back up your VCM database business objects and import them into a new VCM database or into a recovered VCM database. This tool also supports the migration of any VCM Management Extension for Asset data that was manually added to VCM.

- "Run the Content Wizard to Access Additional Compliance Content" on page 263

  Use the Content Wizard to import additional VMware content such as VCM Compliance Content Packages.

- "Run the Deployment Utility" on page 263

  The Deployment Utility for UNIX/Linux and ESX/vSphere copies files to multiple target machines when you configure UNIX/Linux and ESX/vSphere machines for management in VCM.

- "Package Studio" on page 264

  Use Package Studio to create software packages that can be installed by VCM.

- "Foundation Checker" on page 264

  Use the Foundation Checker tool to verify that a Windows machine designated as a VCM Collector meets all of the prerequisites necessary to install VCM.

Install the VCM Tools Only

You can install the VCM tools on a non-Collector Windows machine.

If you plan to install VCM on the non-Collector Windows machine later, you must uninstall the tools and then install VCM.

Prerequisites

Perform the installation requirements for each tool in the Advanced Installation selection. For example, you can install Import/Export (I/E) and Content Wizard only on a machine that is running VCM.

Procedure

1. On the non-Collector Windows machine on which you want to install the tools, insert the installation CD.
2. In Installation Manager, click **Run Installation Manager**.

   During the installation, follow the installation requirements that Installation Manager reports when Foundation Checker runs.
3. Complete the initial installation pages, and click **Next** on subsequent pages to access the Select Installation Type page.
   a. Clear the **VMware vCenter Configuration Manager** check box.
   b. Select **Tools**.
   c. To install a subset of tools, clear the **Tools** check box and select only the individual tools to install.
4. Click **Next**.
5. Complete the remaining instructions and click **Next**.
6. On the Installation Complete page, click **Finish**.
7. On the Installation Manager page, click **Exit**.

VCM Import/Export and Content Wizard Tools

Use the Import/Export Tool and the Content Wizard Tool to move or update VCM business objects. These tools support the migration of any VCM Management Extension for Asset data that was added to VCM manually, but does not import or export any collected data.

The Import/Export Tool supports the following scenarios.

- Back up (export) and restore (import) business objects to the same machine.
- Back up (export) and import (if needed) business objects during a VCM upgrade.
- Export and migrate (import) business objects to additional machines in a multi-Collector environment during setup or to move custom content.
- Use the Content Wizard to download current Compliance Content from VMware and import it into an existing database.
- Using the Command Line Interface, automate the propagation of content to other machines in a multi-collector environment with a “golden machine”.
- Aid in disaster recovery by using the Command Line Interface to automate and schedule the backup of VCM content and configuration parameters.

The Command Line Interface (CLI) is a powerful extension of the Import/Export graphic user interface (GUI). In addition to supporting the scenarios noted above, the CLI allows content to be overwritten, as opposed to “rename only”, and provides for automation through scripting suitable for customizations.

IMPORTANT Use of the CLI should be restricted to advanced users who exercise caution when testing their scripts.

The Import/Export Tool and Content Wizard Tool were installed on your Collector machine during your VCM installation. These tools can only be run on a Collector machine.

Run the Import/Export Tool

Use the Import/Export Tool to back up your VCM database business objects and import them into a new VCM database or into a recovered VCM database. This tool also supports the migration of any VCM Management Extension for Asset data that was manually added to VCM.

Prerequisites

Install the Import/Export Tool. See "Installing and Getting Started with VCM Tools" on page 261.

Procedure

1. On the Collector, click **Start**.
2. Select **All Programs > VMware vCenter Configuration Manager > Tools > Import Export Tool**.
3. For importing and exporting procedures, click **Help > Contents** and use the online help.

Run the Content Wizard to Access Additional Compliance Content

Use the Content Wizard to import additional VMware content such as VCM Compliance Content Packages. These packages are not available in VCM until you download and import them. Check the VCM Compliance Content Packages to determine if you need to import them.

Prerequisites

Install the Content Wizard. See "Installing and Getting Started with VCM Tools" on page 261.

Procedure

1. On the Collector, click **Start**.
2. Select **All Programs > VMware vCenter Configuration Manager > Tools > Content Wizard Tool**.
3. In the Content Wizard, select **Get Updates from the Internet** and click **Next**.
4. After the wizard identifies available content, click **Next**.
5. Select the updates to install on your Collector and click **Install**.

   When the installation is finished, the Event Log Results window appears.
6. On the Event Log Results window, click **Save** and specify a location to save the logs.
7. Click **Close**.
8. On the Content Wizard page, click **Exit**.

What to do next

View the imported data in VCM. For example, click **Compliance** and select **Machine Group Compliance > Templates**. You can now run any imported compliance template against your collected data.

Run the Deployment Utility

The Deployment Utility for UNIX/Linux and ESX/vSphere copies files to multiple target machines when you configure UNIX/Linux and ESX/vSphere machines for management in VCM.

Procedure

1. On the Collector, navigate to `C:\Program Files (x86)\VMware\VCM\Tools`.
2. Copy the `DeployUtility-<version>.zip` file from the Collector to your Windows machine.
3. Extract the files.
4. Double-click `DeployUtil.exe` to start the application.

What to do next

In the Deployment Utility, click Help and review the procedure for the type of machine you are configuring.

Package Studio

Use Package Studio to create software packages that can be installed by VCM.. It is one component of VCM Software Provisioning that includes the Software Repository for Windows and the Package Manager.

For procedures to run the Package Studio, see the *Software Provisioning Components Installation and User's Guide*.

Foundation Checker

Use the Foundation Checker tool to verify that a Windows machine designated as a VCM Collector meets all of the prerequisites necessary to install VCM.

Installation Manager uses VCM Foundation Checker to check a machine's viability for a successful VCM deployment. Foundation Checker runs system checks that determine various conditions, settings, and requirements, and displays a results file that displays the system checks that passed, failed, or generated warnings.

If the checks run without error, you can install VCM. If the checks identify missing components or incorrect configurations, Foundation Checker instructs you where to verify the component or configuration and how to remedy the errors.

To run the Foundation Checker on a Windows machine on which you will install another instance of VCM, see the *Foundation Checker User's Guide*.

Index

%

%Systemroot% environment variable **85**, **87**

A

About Patching **181**
about this book **9**
access by user **71**
accessing
  compliance content **263**
account
  application services **14**
  collector services **13**
  network authority **12**
active directory
  (AD) **249**
  collection results **258**
  configuration **255**
  data collection **258**
  getting started **249**
  installing VCM for active directory **255**
  run determine forest action **256**
  run domain controller setup action **256**
AD (active directory) **249**
adding
  asset data field **236**
  hardware asset data **240**
  Mac OS X **123**
  multiple hardware asset data **241**
  multiple software asset data **244**
  Oracle Instances **133-134**
  repository sources **227**
  software asset data **243**
  UNIX/Linux machines **112**
administration
  rights **12**
ADProductInstall.exe for Windows **85**, **87**
agent
  ADProductInstall.exe for Windows AD **85**, **87**
  CMAgentInstall.exe for Windows **85**, **87**
  installation **16**, **83**
  installation, manually **84**
  installing
    Mac OS X **124**
  platforms supported **57**
  proxy
    upgrading **60**
    upgrading manually **61**
  uninstall, Mac OS X **129**
  uninstall, UNIX/Linux **120**
  uninstalling **88**
  UNIX upgrade **57**, **59**
  upgrading **55**
  upgrading for UNIX **57**
agent communication
  changing after OS provisioning **211**
agents
  certificates **15**
AgentUpgradeLocal.sh for UNIX **58**
application services
  account **14**
assets
  adding data field **236**
  adding hardware data **240**
  adding multiple hardware data **241**
  adding multiple software data **244**
  adding software data **243**
  deleting data field **238**
  deleting hardware data **242**
  deleting software data **246**
  editing hardware data **241**
  editing hardware data values **242**
  editing software data **245**
  editing software data values **245**
  edting data field **237**
  getting started **235**
  rearranging data fields **238**
  refreshing dynamic data field **239**
  reviewing data fields **236**
assigning
  network authority account **79**
auditing **139**
authentication
  server **14**
automatic upgrade
  Remote client **56**

B

backup/disaster recovery plan **70**
basicimport
  provisioning, operating system **38**
binary mode, use for ftp **115**, **125**
boot image,Windows
  provisioning, operating system **27**
broadband **167**

C

certificates
  agents **15**
  collector **15**
  enterprise **15**
  secure communication **14**

certificates,copy
provisioning, operating system **27**
change detection
WCI **103**
check
for UNIX/Linux updates **192**
for Windows updates **185**
checking
network authority account **78**, **250**
CMAgentInstall.exe
for Windows **85**, **87**
uninstalling agent **88**
collect
package managers **226**
repositories **226**
vCloud Director
vApp **152**, **158**
collect distributions
provisioning, operating system **201**
collection results
active directory **258**
Oracle **138**
Remote **179**
UNIX/Linux **121**
virtualization **152**
collection scripts
custom for WCI **105**
collection user account
creating, Config User Action **136**
collections
active directory **258**
domain controllers **254**
Mac OS X **129**
Oracle **137**
patching **185**
results, Mac OS X **131**
troubleshooting vCenter Server **146**
UNIX/Linux **121**
vCenter Server data **143**, **145-146**
virtualization **151**
WCI **106**
Windows machines **90**
collector
aware of Remote client **168**, **178**
certificates **15**
install before agents **115**, **125**
lock request **86**
collector services
account **13**
compliance
checking, UNIX/Linux **121**
content, accessing **263**
Mac OS X **131**
rule
remediation
software provisioning **232**
software provisioning **231**
configuration
Active Directory **255**
configurations
database file growth **67**
configure
provisioning, operating system **21**
configuring
vSphere Client Plug-in **164**
content for compliance **263**
wizard **262**
copying
files to ESX/vSphere servers **150**
creating
Oracle collection user account **136**
credentials
vCloud Director
vApp **155**
CSI_AGENT_RUN_OPTION **115**, **125**
custom filter sets
for Remote **169**
customization
component settings **65**
for your environment **139**

D

database
backup/disaster recovery plan **70**
recovery settings **68**
deleting
asset data field **238**
hardware asset data **242**
software asset data **246**
deploying
patches, UNIX/Linux **196**
patches, Windows machines **190**
determine forest action
running for active directory **256**
developing
custom collection scripts **105**
DHCP
provisioning, operating system **25**
dialup **167**
disabling
UAC on Windows machines **81**
disaster recovery plan **70**
discover
vCloud Director
vApp **158**
discovering
domain controllers **249**, **251**
Oracle Instances **132**
Windows machines **77**, **79**
discovery
provisioning, operating system **202**
distributions
provisioning, operating system **201**
domain controllers
collecting **254**

discover, license, install **249**
discovering **251**
domain discovery **250**
licensing **252**
run setup action **256**
domain discovery
domain controllers **250**
Windows machines **78**
domains
active directory **249**
download settings
patch assessment content **184**

E

editing
asset data field **237**
hardware asset data **241**
hardware asset data values **242**
software asset data **245**
software asset data values **245**
VCM asset data **239**
enabling
UAC on Windows machines **89**
enterprise
certificates **15**
environment variable, %Systemroot% **85**, **87**
esx
provisioning, operating system **213**
ESX and ESXi
configure after provisioning **213**
ESXi **142**
exploring
assessment results, UNIX **194**
assessment results, Windows **187**
collection results
Oracle **138**
UNIX/Linux **121**
virtualization **152**
Remote collection results **179**

F

filter sets
Remote **169**
filters
vCloud Director
vApp
collect **156**
forest
run determine forest action **256**
forests
active directory **249**
foundation checker **261**
installation **264**
ftp, use binary mode **115**, **125**

G

getting started **77**
active directory **249**
assets **235**
auditing **139**
deploy patches, UNIX/Linux **196**
deploy patches, Windows **190**
explore assessment results, UNIX **194**
explore assessment results, Windows **187**
launch assessment **186**
launching **72**
logging on **72**
patching collection **185**
Remote **167**
tools **261**
virtualization **141**
vSphere Client Plug-in **165**
WCI **92**
WCI PowerShell scripts **94**
Getting Started
Using Patching **184**

H

HTTP agent, port number **86**

I

import
distributions
provisioning, operating system **33**
Windows directories **34**
provisioning, operating system
Linux/ESX **36**
Windows
provisioning, operating system **34**
import/export wizard **262**
importing
provisioning, operating system
basicimport **38**
information bar in portal **73**
install
provisioning, operating system **21-22**
installation
agent **16**
agent on Mac OS X machines **124**
agent on Red Hat, SUSE **115**
agent on UNIX/Linux machines **114**
agent on Windows machines **83**
agent, manually **84**
agent, UNIX **115**, **125**
check prerequisites **12**
foundation checker **264**
maintenance after **65**
navigating **19**
preparing **11**
prerequisites **12**
Remote client
command line **172-173**
remote command **172**, **175**
tools **12**, **261**
using installation manager **11**
Windows machines **77**, **249**

InstallCMAgent **116**, **126**
installing
Package Manager for Windows **222**
Package Studio **220**
packages **228**
repositories **219**
VCM for active directory **255**
integration
provisioning, operating system
stunnel **29-30**, **32**
Service Desk **247**
integraton, stunnel
provisioning, operating system **28**
invalid certificate in vSphere Client
troubleshooting **166**

J
job manager **261**
job status reporting
WCI **108**
jobs history
provisioning **230**

L
LAN **167**
launch an assessment **186**
licensing
domain controllers **249**, **252**
Mac OS X **124**
UNIX/Linux machines **114**
Windows machines **77**, **80**
Linux/ESX
provisioning, operating system
import **36**
local package
UNIX agent upgrade **57**
lock request, submit from collector **86**
logs
provisioning, operating system **40**

M
Mac OS X
adding **123**
agent
installing **124**
agent, uninstall **129**
collection **129**
collection results **131**
licensing **124**
maintenance
after installation **65**
backup/disaster recovery plan **70**
configure database file growth **67**
create plan **69**
customize settings **65**
database recovery settings **68**
migrating **43**
migration prerequisites **44**, **46**

N
NAT
see network address translation **153**
network address translation
vCloud Director
vApp **153**
network authority account **12**
assigning **79**
checking **78**, **250**

O
Oracle
10g installations **136**
Add/Edit Instance **131**
adding instances **133-134**
collection results **138**
collection user account **136**
collections **137**
Config User Action **136**
discovering instances **132**
permissions **136**
ospctl commands
provisioning, operating system **40**
overview
vSphere Client Plug-in **163**

P
Package Manager for Windows
installing **222**
package managers
collect **226**
Package Studio
installing **220**
packages
installing **228**
password
provisioning, operating system
vcmuser **24**
patch assessment content architecture
download settings **184**
repository **184**
patching
check for updates, UNIX/Linux **192**
check for updates, Windows **185**
collection **185**
permissions
Oracle **136**
planning maintenance **69**
platforms
UNIX agent support **57**
port number for HTTP agent install **86**
port number for UNIX agent install **118**, **127**
portal
familiarizing **73**
information bar **73**
sliders **75**
toolbar **74**

PowerShell
executing for WCI **98**
for Windows Custom Info **106**
scripts, troubleshooting **111**
signing scripts for WCI **98**
WCI getting started **94**
prerequisites
check for installation **12**
for migration **46**
vCenter Server collections **143**
prerequisites for migration **44**
Product Overview **181**
provision machines
operating systems **202-203**, **205**, **211**
provisioning
compliance
remediation **232**
compliance rule **231**
install agent **16**
jobs History **230**
provisioning, operating system **199**
agent communication **211**
certificates,copy **27**
collect distributions **201**
components **199**
confgure **21**
configure **21**
configure ESX and ESXi **213**
DHCP **25**
discovery **202**
distributions **201**
importing **33**
esx **213**
import
Linux/ESX **36**
Windows **34**
importing
basicimport **38**
create Windows directories **34**
install **21-22**
integration
stunnel **28**
Linux
time **210**
logs **40**
ospctl commands **40**
provision machines **202-203**, **205**, **211**
re-provision machines **214**
results **214**
set vcmuser password **24**
stunnel **29-30**, **32**
TFTP **26**
uninstall **24**
upgrade **39**
Windows boot image **27**
workflow **200**
purge
for WCI **107**

R

re-provisioning machines
operating systems **214**
rearranging
asset data fields **238**
recovery plan **70**
Red Hat
install UNIX agent **115**
refreshing
dynamic asset data field **239**
registering
vSphere Client Plug-in **63**, **163**
remediation
compliance rule
software provisioning **232**
Remote
collection results **179**
filter sets **169**
getting started **167**
settings **168**
virtual directory **14**
Remote client
automatic upgrade **56**
collector aware **168**, **178**
installing
command line **172-173**
remote command **172**, **175**
remote package
UNIX agent upgrade **59**
repairing
uninstall, troubleshooting **19**
reports
WCI **110**
repositories
collect **226**
installing **219**
repository for patch assessment content **184**
repository sources
adding **227**
results
collection, active directory **258**
collection, Mac OS X **131**
provisioning, operating system **214**
vCloud Director
vApp **162**
virtualization **152**
reviewing
asset data fields **236**
rights
administration **12**
running
determine forest action **256**
domain controller setup **256**

S

scripts
PowerShell **94**
secure communication **14**

server
authentication **14**
Service Desk integration **247**
settings
cusomizing for components **65**
database recovery **68**
remote **168**
setup action
running for active directory **256**
signing
PowerShell scripts **98**
sliders
in portal **75**
sources
repository sources
adding **227**
SQL*Plus
Oracle **136**
stunnel
provisioning, operating system **28-30**, **32**
SUSE
install UNIX agent **115**

T

TFTP
provisioning, operating system **26**
time
provisioning, operating system
Linux **210**
ToCMBase64String **94**
toolbar
in portal **74**
tools
foundation checker **261**
getting started **261**
import/export, content **261**
installation **12**, **261**
job manager **261**
troubleshooting
PowerShell scripts **111**
vCenter Server data collections **146**
vSphere client integration **166**

U

UAC
disabling on Windows machines **81**
enabling on Windows machines **89**
uninstall
agent **88**
agent, Mac OS X **129**
agent, UNIX/Linux **120**
provisioning, operating system **24**
troubleshooting **19**
UNIX agent
platform support **57**
port number **118**, **127**
upgrading **57**
local package **57**
remote package **59**
UNIX patch assessment content repository **184**
UNIX patch content download **184**
UNIX/Linux
agent uninstall **120**
AgentUpgradeLocal.sh **58**
check for updates **192**
collections **121**
machines, adding **112**
machines, licensing **114**
updates
check for UNIX/Linux **192**
check for Windows **185**
upgrade
provisioning, operating system **39**
upgrading **43**
agent **55**
agent proxy **60**
agent proxy manually **61**
failed, troubleshooting **19**
UNIX agent **57**
local package **57**
remote package **59**
virtualization **60**
vSphere Client Plug-in **63**
user access **71**

V

vCenter Server **143**
data collections **143**, **145**
vCloud Director
vApp
collect **152**, **158**
credentials **155**
filters **156**
discover **158**
network address translation **153**
results **162**
VCM actions tab; troubleshooting **166**
VCM asset data
editing **239**
VCM Summary and VCM Action
troubleshooting **166**
VCM summary tab
troubleshooting **166**
virtual directory
Remote **14**
virtual machines
collect
vCloud Director
vApp **152**
virtualization
collecting **151**
results **152**
collections **151**
getting started **141**
upgrading **60**

vSphere Client Plug-in
configuring **164**
getting started **165**
overview **163**
registering **163**
upgrading **63**

W

WCI
change detection **103**
collection **106**
custom collection scripts **105**
executing PowerShell scripts **98**
getting started **92**
job status reporting **108**
purge **107**
running reports **110**
Windows
check for updates **185**
import
provisioning, operating system **34**
Windows boot image
provisioning, operating system **27**
Windows Custom Information (WCI) **92**
Windows directories
provisioning, operating system
import **34**
Windows machines
collecting **90**
disabling UAC **81**
discover, license, install **77**
discovering **79**
domain discovery **78**
enabling UAC **89**
install agent **83**
licensing **80**
uninstalling agent **88**
wizards
content **262**
import/export **262**